Systemverwaltungshandbuch: IP Services

Teilenr.: 820–2980–17
September 2010

100916@24661

Inhalt

Vorwort ... 29

Teil I **Einführung in die Systemverwaltung: IP Services** ... 35

1 **Oracle Solaris TCP/IP-Protokollfamilie (Übersicht)** ... 37
Neuheiten in dieser Version ... 37
Einführung in die TCP/IP-Protokollfamilie ... 37
Protokollschichten und das Open Systems Interconnection-Modell ... 38
Modell der TCP/IP-Protokollarchitektur ... 39
So verarbeiten TCP/IP-Protokolle die Datenkommunikation ... 45
Datenkapselung und der TCP/IP-Protokollstapel ... 45
TCP/IP Internal Trace-Unterstützung ... 49
Weitere Informationen zu TCP/IP und dem Internet ... 49
Computerbücher über TCP/IP ... 49
Websites zum Thema TCP/IP und Arbeiten in Netzwerken ... 50
Requests for Comments und Internet Drafts ... 50

Teil II **Administration von TCP/IP** ... 53

2 **Planen Ihres TCP/IP-Netzwerks (Vorgehen)** ... 55
Netzwerkplanung (Übersicht der Schritte) ... 55
Festlegen der Netzwerkhardware ... 57
Festlegen eines IP-Adressierungsformats für Ihr Netzwerk ... 58
IPv4-Adressen ... 58
IPv4-Adressen im CIDR-Format ... 59
DHCP-Adressen ... 59
IPv6-Adressen ... 59

Private Adressen und Dokumentationspräfixe 59
Beziehen der IP-Adresse Ihres Netzwerks 60
Erstellen eines IPv4-Adressierungsschemas 61
Erstellen eines IPv4-Adressierungsschemas 62
IPv4-Teilnetznummer 63
Erstellen eines CIDR IPv4-Adressierungsschemas 64
Verwenden privater IPv4-Adressen 65
Anwenden von IP-Adressen für Netzwerkschnittstellen 65
Benennen von Entitäten in Ihrem Netzwerk 66
Verwalten von Hostnamen 66
Auswählen eines Namen- und Verzeichnisservices 67
Planen der Router für Ihr Netzwerk 69
Einführung in die Netzwerktopologie 69
So übertragen Router Pakete 71

3 Einführung in IPv6 (Überblick) 73
Die wichtigsten Leistungsmerkmale von IPv6 74
Erweiterte Adressierung 74
Automatische Adresskonfiguration und Neighbor Discovery 74
Vereinfachung des Header-Formats 74
Verbesserte Unterstützung für IP-Header-Optionen 75
Anwendungsunterstützung für IPv6-Adressierung 75
Weitere IPv6-Ressourcen 75
Einführung in IPv6-Netzwerke 76
Einführung in die IPv6-Adressierung 78
Komponenten einer IPv6-Adresse 79
Abkürzen von IPv6-Adressen 80
Präfixe in IPv6 80
Unicast-Adressen 81
Multicast-Adressen 83
Anycast-Adressen und -gruppen 84
Einführung in das IPv6 Neighbor Discovery-Protokoll 84
Automatische IPv6-Adresskonfiguration 86
Einführung in die statusfreie automatische Konfiguration 86
Einführung in IPv6-Tunnel 87

4 Planen eines IPv6-Netzwerks (Aufgaben) ... 89

Planung der Einführung von IPv6 (Übersicht der Schritte) ... 89

Szenario einer IPv6-Netzwerktopologie ... 91

Vorbereiten eines bestehenden Netzwerks zur Unterstützung von IPv6 ... 93

Vorbereiten der Netzwerktopologie auf die Unterstützung von IPv6 ... 93

Vorbereiten der Netzwerkservices auf die Unterstützung von IPv6 ... 94

Vorbereiten von Servern auf die Unterstützung von IPv6 ... 94

▼ So bereiten Sie Netzwerkservices auf die Unterstützung von IPv6 vor ... 95

▼ So bereiten Sie das DNS auf die Unterstützung von IPv6 vor ... 96

Planung für Tunnel in der Netzwerktopologie ... 96

Sicherheitsbetrachtungen bei der Einführung von IPv6 ... 97

Vorbereiten eines IPv6-Adressierungsplans ... 98

Beziehen eines Standortpräfix ... 98

Erstellen eines IPv6-Nummerierungsschemas ... 98

5 Konfiguration der TCP/IP-Netzwerkservices und IPv4-Adressierung (Aufgaben) ... 101

Neuerungen in diesem Kapitel ... 102

Vor der Konfiguration eines IPv6-Netzwerks (Übersicht der Schritte) ... 102

Festlegen der Host-Konfigurationsmodi ... 103

Systeme, die im lokale Dateien-Modus ausgeführt werden sollten ... 104

Als Netzwerkclients konfigurierte Systeme ... 105

Gemischte Konfigurationen ... 105

IPv4-Netzwerktopologie – Szenario ... 105

Hinzufügen eines Teilnetzes zu einem Netzwerk (Übersicht der Schritte) ... 106

Netzwerkkonfiguration (Übersicht der Schritte) ... 107

Konfiguration der Systeme im lokalen Netzwerk. ... 108

▼ So konfigurieren Sie einen Host für den lokale Dateien-Modus ... 109

▼ So richten Sie einen Netzwerkkonfigurationsserver ein ... 112

Konfiguration der Netzwerkclients ... 113

▼ So konfigurieren Sie Hosts für den Netzwerkclient-Modus ... 113

▼ So ändern Sie die IPv4-Adresse und andere Netzwerkkonfigurationsparameter ... 114

Paketweiterleitung und Routing bei IPv4-Netzwerken ... 119

Von Oracle Solaris unterstützte Routing-Protokolle; ... 120

Topologie eines autonomen IPv4-Systems ... 123

Konfiguration eines IPv4-Routers ... 126

Routing-Tabellen und Routing-Typen 131
Konfiguration von Multihomed-Hosts 134
Konfiguration des Routings auf Systemen mit einer Schnittstelle 138
Überwachen undModifizieren der Transportschichtservices 142
▼ So protokollieren Sie die IP-Adressen aller eingehenden TCP-Verbindungen 143
▼ So fügen Sie Services hinzu, die das SCTP-Protokoll verwenden 143
▼ So verwenden Sie TCP-Wrapper zur Kontrolle des Zugriffs auf TCP-Services 147
Verwalten der Schnittstellen in Solaris 10 3/05 147
Neuerungen in diesem Abschnitt 148
Konfiguration physikalischer Schnittstellen unter Solaris 10 3/05 148
Konfiguration von VLANs (nur Solaris 10 3/05) 152

6 Verwalten von Netzwerkschnittstellen (Aufgaben) 155
Neuerungen bei der Verwaltung von Netzwerkschnittstellen 155
Schnittstellenverwaltung (Übersicht der Schritte) 156
Grundlagen zur Verwaltung physikalischer Schnittstellen 157
▼ So beziehen Sie den Schnittstellenstatus 157
▼ So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation 159
▼ So entfernen Sie eine physikalische Schnittstelle 162
▼ SPARC: So stellen Sie sicher, dass die MAC-Adresse einer Schnittstelle einmalig ist 163
Grundlagen zur Verwaltung physikalischer Schnittstellen 165
Netzwerkschnittstellennamen 165
Plumben (aktivieren) einer Schnittstelle 166
Oracle Solaris-Schnittstellentypen 166
Verwalten von virtuellen lokalen Netzwerken 167
Einführung in die VLAN-Topologie 167
Planen von VLANs in einem Netzwerk 170
Konfiguration von VLANs 171
Übersicht der Link-Aggregationen 173
Grundlagen der Linkaggregationen 173
Back-to-Back Linkaggregationen 175
Richtlinien und Lastenausgleich 176
Aggregationsmodi und Switches 176
Anforderungen für Linkaggregationen 177
▼ So erstellen Sie eine Linkaggregation 177

▼ So bearbeiten Sie eine Aggregation ... 179
▼ So entfernen Sie eine Schnittstelle aus einer Aggregation ... 181
▼ So löschen Sie eine Aggregation ... 181
▼ So konfigurieren Sie VLANs über eine Linkaggregation ... 182

7 Konfigurieren eines IPv6-Netzwerks (Vorgehen) ... 185

Konfiguration einer IPv6-Schnittstelle ... 185
Aktivieren von IPv6 auf einer Schnittstelle (Übersicht der Schritte) ... 186
▼ So aktivieren Sie eine IPv6-Schnittstelle für die aktuelle Sitzung ... 186
▼ So aktivieren Sie persistente IPv6-Schnittstellen ... 188
▼ So deaktivieren Sie die automatische IPv6-Adresskonfiguration ... 190
Konfiguration eines IPv6-Routers ... 191
Konfiguration eines IPv6-Routers (Übersicht der Schritte) ... 191
▼ So konfigurieren Sie einen IPv6-konformen Router ... 192
Modifizieren einer IPv6-Schnittstellenkonfiguration für Hosts und Server ... 196
Ändern einer IPv6-Schnittstellenkonfiguration (Übersicht der Schritte) ... 196
Verwenden von temporären Adressen für eine Schnittstelle ... 196
Konfiguration eines IPv6-Tokens ... 200
Verwaltung von IPv6-konformen Schnittstellen auf Servern ... 202
Aufgaben bei der Konfiguration von Tunneln zur Unterstützung von IPv6 (Übersicht der Schritte) ... 204
Konfiguration von Tunneln zur Unterstützung von IPv6 ... 205
▼ So konfigurieren Sie einen IPv6-über-IPv4-Tunnel ... 205
▼ So konfigurieren Sie einen IPv6-über-IPv6-Tunnel ... 206
▼ So konfigurieren Sie einen IPv4-über-IPv6-Tunnel ... 207
▼ So konfigurieren Sie einen 6to4-Tunnel ... 208
▼ So konfigurieren Sie einen 6to4-Tunnel zu einem 6to4-Relay-Router ... 211
Konfiguration der Namen-Services-Unterstützung für IPv6 ... 213
▼ So fügen Sie IPv6-Adressen zum DNS hinzu ... 214
Hinzufügen von IPv6-Adressen zum NIS ... 214
▼ So zeigen Sie Informationen zum IPv6-Namen-Service an ... 215
▼ So prüfen Sie, ob die DNS IPv6 PTR-Datensätze korrekt aktualisiert wurden ... 216
▼ So zeigen Sie IPv6-Informationen über NIS an ... 216
▼ So zeigen Sie IPv6-Informationen unabhängig vom Namen-Service an ... 217

8 Verwaltung eines TCP/IP-Netzwerks (Aufgaben) 219

Aufgaben bei der Verwaltung von TCP/IP Netzwerken (Übersicht der Schritte) 220

Überwachen der Schnittstellenkonfiguration mit dem Befehl `ifconfig` 221

▼ So zeigen Sie Informationen zu einer bestimmten Schnittstelle an 221

▼ So zeigen Sie die Schnittstellen-Adresszuweisungen an 223

Überwachen des Netzwerkstatus mit dem Befehl `netstat` 225

▼ So zeigen Sie Statistiken nach dem Protokoll an 226

▼ So zeigen Sie den Status von Transportprotokollen an 227

▼ So zeigen Sie den Netzwerkschnittstellenstatus an 228

▼ So zeigen Sie den Status der Sockets an 229

▼ So zeigen Sie den Status von Paketübertragungen eines bestimmten Adresstyps an 230

▼ So zeigen Sie den Status bekannter Routen an 231

Ermitteln des Status von Remote-Hosts mit dem Befehl `ping` 232

▼ So ermitteln Sie, ob ein Remote-Host ausgeführt wird 232

▼ So stellen Sie fest, ob ein Host Pakete abwirft 233

Verwalten und Protokollieren der Netzwerkstatusanzeigen 234

▼ So steuern Sie die Anzeige der Ausgabe von IP-bezogenen Befehlen 234

▼ So protokollieren Sie die Aktionen des IPv4-Routing-Daemon 235

▼ So verfolgen Sie die Aktivitäten des IPv6 Neighbor Discovery-Daemon 236

Anzeigen von Routing-Informationen mit dem Befehl `traceroute` 237

▼ So ermitteln Sie die Route zu einem Remote-Host 237

▼ So verfolgen Sie alle Routen 238

Überwachen der Paketübertragungen mit dem Befehl `snoop` 238

▼ So prüfen Sie Pakete von allen Schnittstellen 239

▼ So erfassen Sie die Ausgabe des Befehls `snoop` in einer Datei 240

▼ So prüfen Sie Pakete zwischen einem IPv4-Server und einem Client 241

▼ So überwachen Sie den IPv6-Netzwerkverkehr 241

Verwaltuen der standardmäßigen Adressauswahl 242

▼ So verwalten Sie die Richtlinientabelle zur IPv6-Adressauswahl 243

▼ So modifizieren Sie die IPv6-Adressauswahltabelle nur für die aktuelle Sitzung 244

9 Fehlersuche bei Netzwerkproblemen (Aufgaben) 247

Neuerungen in diesem Kapitel 247

Allgemeine Tipps zur Fehlersuche bei Netzwerkproblemen 247

Durchführen allgemeiner Diagnoseprüfungen 248

▼ So führen Sie eine allgemeine Prüfung der Netzwerksoftware durch 248
Allgemeine Probleme bei der Bereitstellung von IPv6 249
IPv4-Router kann nicht auf IPv6 aufgerüstet werden 249
Probleme beim Aufrüsten von Services auf IPv6 249
Der aktuelle ISP unterstützt IPv6 nicht 249
Sicherheitsbetrachtungen beim Tunneling zu einem 6to4-Relay-Router 250
Bekannte Probleme bei einem 6to4-Router 251

10 TCP/IP und IPv4 im Detail (Referenz) 253
Neuerungen in diesem Kapitel 253
TCP/IP-Konfigurationsdateien 253
`/etc/hostname.`*Schnittstelle*-Datei 254
`/etc/nodename`-Datei 255
`/etc/defaultdomain`-Datei 255
`/etc/defaultrouter`-Datei 255
`hosts`-Datenbank 255
`ipnodes`-Datenbank 259
`netmasks`-Datenbank 260
`inetd` Internet Services-Daemon 263
Netzwerkdatenbanken und die `nsswitch.conf`-Datei 264
Auswirkungen der Namen-Services auf Netzwerkdatenbanken 265
`nsswitch.conf`-Datei 267
`bootparams`-Datenbank 269
`ethers`-Datenbank 270
Andere Netzwerkdatenbanken 271
`protocols`-Datenbank 272
`Services`-Datenbank 272
Routing-Protokolle in Oracle Solaris 273
Routing Information Protocol (RIP) 273
ICMP Router Discovery (RDISC)-Protokoll 274
Netzwerkklassen 274
Klasse A-Netzwerknummern 274
Klasse B-Netzwerknummern 275
Klasse C-Netzwerknummern 275

11 IPv6 im Detail (Referenz) ... 277
Neuerungen in diesem Kapitel ... 277
Weiterführende IPv6-Adressierungsformate ... 278
Von 6to4 abgeleitete Adressen ... 278
IPv6-Multicast-Adressen im Detail ... 280
Format der IPv6-Paket-Header ... 281
IPv6-Extension-Header ... 282
Dual-Stack-Protokolle ... 283
Oracle Solaris 10 IPv6-Implementierung ... 284
IPv6-Konfigurationsdateien ... 284
IPv6-bezogene Befehle ... 289
IPv6-bezogene Daemons ... 295
IPv6 Neighbor Discovery-Protokoll ... 299
ICMP-Nachrichten im Neighbor Discovery-Protokoll ... 299
Automatische Konfiguration ... 300
Neighbor Solicitation und Unerreichbarkeit ... 302
Algorithmus zur Erkennung doppelt vorhandener Adressen ... 303
Proxy Advertisement-Nachrichten ... 303
Lastausgleich für eingehende Daten ... 303
Ändern einer Link-lokalen Adresse ... 304
Vergleich von Neighbor Discovery mit ARP und verwandten IPv4-Protokollen ... 304
IPv6-Routing ... 306
Router Advertisement-Nachrichten ... 307
IPv6-Tunnel ... 308
Konfigurierte Tunnel ... 309
Automatische 6to4-Tunnel ... 312
IPv6-Erweiterungen zu den Oracle Solaris-Namen-Services ... 316
DNS-Erweiterungen für IPv6 ... 316
Änderungen an der `nsswitch.conf`-Datei ... 316
Änderungen an den Namen-Service-Befehlen ... 318
NFS und RPC IPv6-Unterstützung ... 318
Unterstützung für IPv6-über-ATM ... 318

Teil III DHCP ... 319

12 Einführung in Oracle Solaris DHCP ... 321
Einführung in das DHCP-Protokoll ... 321
Vorteile der Verwendung von Oracle Solaris DHCP ... 322
Arbeitsweise des DHCP-Protokolls ... 323
Oracle Solaris DHCP-Server ... 326
Verwaltung eines DHCP-Servers ... 327
DHCP-Datenspeicher ... 327
DHCP Manager ... 329
DHCP-Befehlszeilenprogramme ... 330
Rollenbasierte Zugriffskontrolle für DHCP-Befehle ... 331
Konfiguration eines DHCP-Servers ... 332
Zuweisung von IP-Adressen ... 333
Netzwerkkonfigurationsinformationen ... 333
Einführung in DHCP-Optionen ... 333
Einführung in DHCP-Makros ... 334
Oracle Solaris DHCP-Client ... 336

13 Planungen für den DHCP-Service (Aufgaben) ... 337
Vorbereiten Ihres Netzwerks für den DHCP-Service (Übersicht der Schritte) ... 337
Erstellen einer Netzwerktopologie ... 338
Festlegen der Anzahl von DHCP-Servern ... 339
Aktualisieren von Systemdateien und Netzmasken-Tabellen ... 340
Entscheidungen bei der Konfiguration Ihres DHCP-Servers (Übersicht der Schritte) ... 342
Auswählen eines Hosts zum Ausführen des DHCP-Services ... 343
Auswählen des DHCP-Datenspeichers ... 343
Einrichten einer Leasing-Richtlinie ... 345
Festlegen der Router für DHCP-Clients ... 346
Entscheidungen bei der Verwaltung von IP-Adressen (Übersicht der Schritte) ... 346
Anzahl und Bereiche der IP-Adressen ... 347
Erzeugung des Client-Hostnamen ... 347
Standardmäßige Client-Konfigurationsmakros ... 348
Dynamische und permanente Leasing-Typen ... 349
Reservierte IP-Adressen und Leasing-Typ ... 350

Planung für mehrere DHCP-Server ... 350
Planung einer DHCP-Konfiguration für remote Netzwerke ... 351
Auswählen des Tools zur Konfiguration von DHCP ... 351
Funktionen von DHCP Manager ... 352
`dhcpconfig`-Funktionen ... 352
Vergleich von DHCP Manager und `dhcpconfig` ... 353

14 Konfiguration des DHCP-Services (Aufgaben) ... 355
Konfigurieren und Dekonfigurieren eines DHCP-Servers mithilfe von DHCP Manager ... 356
Konfiguration von DHCP-Servern ... 356
▼ So konfigurieren Sie einen DHCP-Server (DHCP Manager) ... 359
Konfiguration eines BOOTP-Relay-Agent ... 360
▼ So konfigurieren Sie einen BOOTP-Relay-Agent (DHCP Manager) ... 361
Dekonfiguration von DHCP-Servern und BOOTP-Relay-Agents ... 361
DHCP-Daten auf einem dekonfigurierten Server ... 362
▼ So dekonfigurieren Sie einen DHCP-Server oder einen BOOTP-Relay-Agent (DHCP Manager) ... 363
Konfigurieren und Dekonfigurieren eines DHCP-Servers mithilfe der `dhcpconfig`-Befehle . 363
▼ So konfigurieren Sie einen DHCP-Server (`dhcpconfig -D`) ... 364
▼ So konfigurieren Sie einen BOOTP-Relay-Agent (`dhcpconfig -R`) ... 365
▼ So dekonfigurieren Sie einen DHCP-Server oder einen BOOTP-Relay-Agent (`dhcpconfig -U`) ... 365

15 Verwalten von DHCP (Aufgaben) ... 367
Allgemeines zum DHCP Manager ... 368
Fenster „DHCP Manager“ ... 368
Menüs in DHCP Manager ... 370
Starten und Stoppen von DHCP Manager ... 370
▼ So starten und stoppen Sie DHCP Manager ... 370
Einrichten des Benutzerzugriffs auf DHCP-Befehle ... 371
▼ So gewähren Sie Benutzern Zugriff auf DHCP-Befehle ... 371
Starten und Stoppen des DHCP-Service ... 372
▼ So starten und stoppen Sie den DHCP-Service (DHCP Manager) ... 373
▼ So aktivieren und deaktivieren Sie den DHCP-Service (DHCP Manager) ... 373
▼ So aktivieren und deaktivieren Sie den DHCP-Service (`dhcpconfig -S`) ... 374

DHCP-Service und die Service Management Facility ... 374
Bearbeiten von DHCP-Service-Optionen (Übersicht der Schritte) ... 375
Ändern der DHCP-Protokollierungsoptionen ... 377
▼ So erzeugen Sie ausführliche DHCP-Protokollmeldungen (DHCP Manager) ... 379
▼ So erzeugen Sie ausführliche DHCP-Protokollmeldungen (Befehlszeile) ... 379
▼ So aktivieren und deaktivieren Sie die DHCP-Transaktionsprotokollierung (DHCP Manager) ... 380
▼ So aktivieren und deaktivieren Sie die DHCP-Transaktionsprotokollierung (Befehlszeile) ... 381
▼ So zeichnen Sie die DHCP-Transaktionen in einer separaten `syslog`-Datei auf ... 381
Aktivieren von dynamischen DNS-Aktualisierungen durch einen DHCP-Server ... 382
▼ So aktivieren Sie die dynamische DNS-Aktualisierung für DHCP-Clients ... 383
Registrierung des Client-Hostnamen ... 385
Anpassen der Leistungsoptionen für den DHCP-Server ... 386
▼ So passen Sie die Optionen für die DHCP-Leistung an (DHCP Manager) ... 387
▼ So passen Sie die Optionen für die DHCP-Leistung an (Befehlszeile) ... 387
Hinzufügen, Modifizieren und Löschen von DHCP-Netzwerken (Übersicht der Schritte) ... 388
Angabe der Netzwerkschnittstellen für die DHCP-Verwaltung ... 389
▼ So geben Sie die Netzwerkschnittstellen an, die unter die DHCP-Verwaltung gestellt werden sollen (DHCP Manager) ... 390
▼ So geben Sie die Netzwerkschnittstellen an, die unter die DHCP-Verwaltung gestellt werden sollen (`dhcpconfig`) ... 391
Hinzufügen von DHCP-Netzwerken ... 391
▼ So fügen Sie ein DHCP-Netzwerk hinzu (DHCP Manager) ... 392
▼ So fügen Sie ein DHCP-Netzwerk hinzu (`dhcpconfig`) ... 393
Ändern der DHCP-Netzwerkkonfigurationen ... 394
▼ So ändern Sie die Konfiguration eines DHCP-Netzwerks (DHCP Manager) ... 395
▼ So ändern Sie die Konfiguration eines DHCP-Netzwerks (`dhtadm`) ... 396
Entfernen von DHCP-Netzwerken ... 397
▼ So löschen Sie ein DHCP-Netzwerk (DHCP Manager) ... 398
▼ So löschen Sie ein DHCP-Netzwerk (`pntadm`) ... 398
Unterstützen von BOOTP-Clients mit dem DHCP-Service (Übersicht der Schritte) ... 399
▼ So richten Sie die Unterstützung für alle BOOTP-Clients ein (DHCP Manager) ... 400
▼ So richten Sie die Unterstützung von registrierten BOOTP-Clients ein (DHCP Manager) ... 401
Arbeiten mit IP-Adressen im DHCP-Service (Übersicht der Schritte) ... 402
Hinzufügen von IP-Adressen zum DHCP-Service ... 406

▼ So fügen Sie eine einzelne IP-Adresse hinzu (DHCP Manager) 408
▼ So duplizieren Sie eine vorhandene IP-Adresse (DHCP Manager) 409
▼ So fügen Sie mehrere IP-Adressen hinzu (DHCP Manager) 409
▼ So fügen Sie IP-Adressen hinzu (`pntadm`) 410
Ändern von IP-Adressen im DHCP-Service 410
▼ So ändern Sie die Eigenschaften von IP-Adressen (DHCP Manager) 412
▼ So ändern Sie die Eigenschaften von IP-Adressen (`pntadm`) 412
Löschen von IP-Adressen aus dem DHCP-Service 413
Kennzeichnen von IP-Adressen als nicht durch den DHCP-Service verwendbar 413
▼ So kennzeichnen Sie IP-Adressen als nicht verwendbar (DHCP Manager) 413
▼ So kennzeichnen Sie IP-Adressen als nicht verwendbar (`pntadm`) 414
Löschen von IP-Adressen vom DHCP-Service 415
▼ So löschen Sie IP-Adressen vom DHCP-Service (DHCP Manager) 415
▼ So löschen Sie IP-Adressen vom DHCP-Service (`pntadm`) 416
Zuweisen einer reservierten IP-Adresse zu einem DHCP-Client 416
▼ So weisen Sie einem DHCP-Client eine konsistente IP-Adresse zu (DHCP Manager) 417
▼ So weisen Sie einem DHCP-Client eine konsistente IP-Adresse zu (`pntadm`) 418
Arbeiten mit DHCP-Makros (Übersicht der Schritte) 419
▼ So zeigen Sie die auf einem DHCP-Server definierten Makros an (DHCP Manager) 421
▼ So zeigen Sie die auf einem DHCP-Server definierten Makros an (`dhtadm`) 421
Ändern von DHCP-Makros 422
▼ So ändern Sie die Werte für Optionen in einem DHCP-Makro (DHCP Manager) 422
▼ So ändern Sie die Werte für Optionen in einem DHCP-Makro (`dhtadm`) 423
▼ So fügen Sie Optionen zu einem DHCP-Makro hinzu (DHCP Manager) 424
▼ So fügen Sie Optionen zu einem DHCP-Makro hinzu (`dhtadm`) 425
▼ So löschen Sie Optionen aus einem DHCP-Makro (DHCP Manager) 425
▼ So löschen Sie Optionen aus einem DHCP-Makro (`dhtadm`) 426
Erstellen von DHCP-Makros 426
▼ So erstellen Sie ein DHCP-Makro (DHCP Manager) 427
▼ So erstellen Sie ein DHCP-Makro (`dhtadm`) 428
Löschen von DHCP-Makros 429
▼ So löschen Sie ein DHCP-Makro (DHCP Manager) 429
▼ So löschen Sie ein DHCP-Makro (`dhtadm`) 429
Arbeiten mit DHCP-Optionen (Übersicht der Schritte) 430
Erstellen von DHCP-Optionen 433
▼ So erstellen Sie DHCP-Optionen (DHCP Manager) 434

▼ So erstellen Sie DHCP-Optionen (`dhtadm`) 435
Ändern von DHCP-Optionen 436
▼ So ändern Sie die Eigenschaften einer DHCP-Option (DHCP Manager) 436
▼ So ändern Sie die Eigenschaften einer DHCP-Option (`dhtadm`) 437
Löschen von DHCP-Optionen 438
▼ So löschen Sie DHCP-Optionen (DHCP Manager) 438
▼ So löschen Sie DHCP-Optionen (`dhtadm`) 439
Ändern der Optionsinformationen eines Oracle Solaris DHCP-Client 439
Unterstützung der Oracle Solaris-Netzwerkinstallation mit dem DHCP-Service 440
Unterstützung von remten Booten und laufwerkslosen Boot-Clients (Übersicht der Schritte) 440
Einrichten von DHCP-Clients ausschließlich zum Empfang von Informationen (Übersicht der Schritte) 442
Umwandeln des DHCP-Datenspeicherstyps 443
▼ So konvertieren Sie den DHCP-Datenspeicher (DHCP Manager) 444
▼ So konvertieren Sie den DHCP-Datenspeicher (`dhcpconfig -C`) 445
Verschieben von Konfigurationsdaten zwischen DHCP-Servern (Übersicht der Schritte) 446
▼ So exportieren Sie Daten aus einem DHCP-Server (DHCP Manager) 448
▼ So exportieren Sie Daten von einem DHCP-Server (`dhcpconfig -X`) 448
▼ So importieren Sie Daten auf einen DHCP-Server (DHCP Manager) 450
▼ So importieren Sie Daten auf einen DHCP-Server (`dhcpconfig -I`) 450
▼ So ändern Sie die importierten DHCP-Daten (DHCP Manager) 451
▼ So ändern Sie importierte DHCP-Daten (`pntadm`, `dhtadm`) 452

16 Konfiguration und Verwaltung des DHCP-Clients 453
Allgemeine Informationen zum Oracle Solaris DHCP-Client 454
DHCPv6-Server 454
Unterschiede zwischen DHCPv4 und DHCPv6 454
Das administrative Modell 455
Protokolldetails 456
Logische Schnittstellen 457
Optionsaushandlung 457
Konfigurationssyntax 457
Start eines DHCP-Clients 458
DHCPv6-Kommunikation 459
So verwalten die DHCP-Client-Protokolle Netzwerkkonfigurationsinformationen 460

Herunterfahren eines DHCP-Clients ... 461
Aktivieren und Deaktivieren eines Oracle Solaris DHCP-Clients ... 462
▼ So aktivieren Sie den Oracle Solaris DHCP-Client ... 462
▼ So deaktivieren Sie einen Oracle Solaris DHCP-Client ... 463
Verwaltung eines DHCP-Client ... 463
`ifconfig`-Befehlsoptionen für den DHCP-Client ... 464
Einrichten der Konfigurationsparameter eines DHCP-Client ... 465
DHCP-Clientsysteme mit mehreren Netzwerkschnittstellen ... 466
Hostnamen für DHCPv4-Clients ... 467
▼ So konfigurieren Sie einen Oracle Solaris DHCPv4-Client zur Anforderung eines bestimmten Hostnamens ... 468
DHCP -Clientsysteme und Namen-Services ... 468
Einrichten von DHCP-Clients als NIS+-Clients ... 470
DHCP-Client Ereignisskripten ... 473

17 DHCP-Fehlerbehebung (Referenz) ... 477
Beheben von Problemen mit dem DHCP-Server ... 477
NIS+-Probleme und der DHCP-Datenspeicher ... 477
Fehler bei der IP-Adresszuweisung unter DHCP ... 481
Troubleshooting DHCP Client Configuration Problems ... 484
Kommunikationsprobleme mit dem DHCP-Server ... 484
Problems With Inaccurate DHCP Configuration Information ... 493
Probleme mit dem vom DHCP-Client angegebenen Hostnamen ... 493

18 DHCP – Befehle und Dateien (Referenz) ... 497
DHCP-Befehle ... 497
Ausführen von DHCP-Befehlen in Skripten ... 498
Vom DHCP-Service verwendete Dateien ... 504
DHCP-Optionsinformationen ... 506
Feststellen, ob Ihr Standort betroffen ist ... 506
Unterschiede zwischen den Dateien `dhcptags` und `inittab` ... 507
Umwandeln von `dhcptags`-Einträgen zu `inittab`-Einträgen ... 508

Teil IV IP-Sicherheit 509

19 IP Security Architecture (Übersicht) 511
Neuerungen in IPsec 511
Einführung in IPsec 513
IPsec RFCs 514
IPsec-Terminologie 515
IPsec-Paketfluss 516
IPsec und Sicherheitszuordnungen 519
Schlüsselmanagement in IPsec 519
IPsec-Schutzmechanismen 520
Authentication Header 520
Encapsulating Security Payload 521
Authentifizierungs- und Verschlüsselungsalgorithmen in IPsec 522
IPsec-Schutzrichtlinien 524
Transport- und Tunnelmodi in IPsec 525
Virtuelle private Netzwerke und IPsec 527
IPsec und NAT Traversal 528
IPsec und SCTP 529
IPsec und Solaris Zones 529
IPsec und Logische Domains 530
IPsec-Dienstprogramme und Dateien 530
Änderungen an IPsec für Solaris 10 532

20 Konfiguration von IPsec (Aufgaben) 533
Schützen des Datenverkehrs mit IPsec (Übersicht der Schritte) 533
Schützen von Datenverkehr mit IPsec 534
▼ So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec 535
▼ How to Use IPsec to Protect a Web Server From Nonweb Traffic 539
▼ So zeigen Sie die IPsec-Richtlinien an 542
▼ So erzeugen Sie Zufallszahlen auf einem Solaris-System 543
▼ So erstellen Sie manuell IPsec-Sicherheitszuordnungen 545
▼ So prüfen Sie, ob Pakete mit IPsec geschützt sind 550
▼ How to Configure a Role for Network Security 551
▼ Verwalten von IKE- und IPsec-Services 553

Schützen eines VPN mit IPsec 554
Beispiele für den Schutz eines VPN mit IPsec mithilfe von Tunneln im Tunnelmodus 555
Schützen eines VPN mit IPsec (Übersicht der Schritte) 557
Beschreibung der Netzwerktopologie für IPsec-Aufgaben zum Schützen eines VPN 558
▼ So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4 560
▼ So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv6 570
▼ So schützen Sie ein VPN mit einem IPsec-Tunnel im Transportmodus über IPv4 576
▼ So schützen Sie ein VPN mit einem IPsec-Tunnel im Transportmodus über IPv6 583
▼ So verhindern Sie IP-Spoofing 589

21 IP Security Architecture (Referenz) 593
IPsec Service Management Facility 593
`ipsecconf`-Befehl 594
`ipsecinit.conf`-Datei 595
Beispiel einer `ipsecinit.conf`-Datei 595
Sicherheitsbetrachtungen für `ipsecinit.conf` und `ipsecconf` 596
`ipsecalgs`-Befehl 597
Sicherheitszuordnung-Datenbank für IPsec 597
Dienstprogramme zur Schlüsselerzeugung in IPsec 598
Sicherheitsbetrachtungen für `ipseckey` 598
IPsec-Erweiterungen für andere Dienstprogramme 599
`ifconfig`-Befehl und IPsec 599
`snoop`-Befehl und IPsec 601

22 Internet Key Exchange (Übersicht) 603
Neuerungen bei IKE 603
Schlüsselmanagement mit IKE 604
IKE-Schlüsselaushandlung 604
IKE-Schlüssel – Terminologie 604
IKE Phase 1 Exchange 605
IKE Phase 2 Exchange 606
IKE-Konfigurationsmöglichkeiten 606
IKE mit PresharedKeys 606
IKE mit PublicKey-Zertifikaten 607
IKE und Hardwarebeschleunigung 608

IKE und Hardware-Speicherung 608
IKE-Dienstprogramme und Dateien 608
Änderungen an IKE für das Release Solaris 10 610

23 Konfiguration von IKE (Aufgaben) 611
Konfiguration von IKE (Übersicht der Schritte) 611
Konfiguration von IKE mit PresharedKeys (Übersicht der Schritte) 612
Konfiguration von IKE mit PresharedKeys 613
▼ So konfigurieren Sie IKE mit PresharedKeys 613
▼ So werden IKE PresharedKeys aktualisiert 616
▼ So rufen Sie IKE PresharedKeys auf 618
▼ So fügen Sie einen IKE PresharedKey für einen neuen Richtlinieneintrag in `ipsecinit.conf` ein 619
▼ So prüfen Sie, ob die IKE PresharedKeys identisch sind 622
Konfiguration von IKE mit PublicKey-Zertifikaten (Übersicht der Schritte) 624
Konfiguration von IKE mit PublicKey-Zertifikaten 624
▼ So konfigurieren Sie IKE mit selbst-signierten PublicKey-Zertifikaten 625
▼ So konfigurieren Sie IKE mit Zertifikaten, die von einer CA signiert wurden 631
▼ So erzeugen Sie PublicKey-Zertifikate und speichern sie auf angehängter Hardware 636
▼ So verarbeiten Sie eine Zertifikat-Rücknahmeliste 640
Konfiguration von IKE für mobile Systeme (Übersicht der Schritte) 642
Konfiguration von IKE für mobile Systeme 643
▼ So konfigurieren Sie IKE für Offsite-Systeme 643
Konfiguration von IKE zum Suchen angehängter Hardware (Übersicht der Schritte) 650
Konfiguration von IKE zum Suchen angehängter Hardware 651
▼ So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 1000-Board 651
▼ So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 4000-Board 652
Ändern der IKE-Übertragungsparameter (Übersicht der Schritte) 654
Ändern der IKE-Übertragungsparameter 654
▼ So ändern Sie die Dauer der Phase 1 IKE-Schlüsselaushandlung 655

24 Internet Key Exchange (Referenz) 657
IKE Service Management Facility 657
IKE-Daemon 658
IKE-Richtliniendatei 658

IKE-Verwaltungsbefehl 659
IKE PresharedKeys-Dateien 660
IKE PublicKey-Datenbanken und -Befehle 660
`ikecert tokens`-Befehl 661
`ikecert certlocal`-Befehl 661
`ikecert certdb`-Befehl 662
`ikecert certrldb`-Befehl 663
`/etc/inet/ike/publickeys`-Verzeichnis 663
`/etc/inet/secret/ike.privatekeys`-Verzeichnis 663
`/etc/inet/ike/crls`-Verzeichnis 664

25 Oracle Solaris IP Filter (Übersicht) 665
Neuerungen bei Oracle Solaris IP Filter 665
Paket Filter-Hooks 665
IPv6-Paketfilterung für Oracle Solaris IP Filter 666
Einführung in Oracle Solaris IP Filter 666
Informationsquellen für Open Source IP Filter 667
Paketverarbeitung mit Oracle Solaris IP Filter 667
Richtlinien zur Verwendung von OpenSolaris IP Filter 670
Verwenden der Oracle Solaris IP Filter-Konfigurationsdateien 670
Arbeiten mit Oracle Solaris IP Filter-Regellisten 671
Verwenden der Paketfilter-Funktionen in Oracle Solaris IP Filter 671
Verwenden der NAT-Funktion in Oracle Solaris IP Filter 674
Verwenden der Adresspool-Funktion in Oracle Solaris IP Filter 675
Paket Filter-Hooks 677
Oracle Solaris IP Filter und das `pfil` STREAMS-Modul 677
IPv6 für Oracle Solaris IP Filter 678
Oracle Solaris IP Filter – Manpages 679

26 Oracle Solaris IP Filter (Aufgaben) 681
Konfiguration von Oracle Solaris IP Filter 681
▼ So aktivieren Sie Oracle Solaris IP Filter 682
▼ So aktivieren Sie Oracle Solaris IP Filter erneut 683
▼ So aktivieren Sie die Loopback-Filterung 684
Deaktivieren und Stoppen von Oracle Solaris IP Filter 685

▼ So deaktivieren Sie die Paketfilterung ... 686
▼ So deaktivieren Sie NAT ... 687
▼ So stoppen Sie die Paketfilterung ... 687
Arbeiten mit dem `pfil`-Modul ... 688
▼ So aktivieren Sie Oracle Solaris IP Filter in älteren Solaris Oracle Solaris-Versionen ... 688
▼ So aktivieren Sie eine NIC für die Paketfilterung ... 691
▼ So deaktivieren Sie Oracle Solaris IP Filter auf einer NIC ... 692
▼ So zeigen Sie die `pfil`-Statistiken für Oracle Solaris IP Filter an ... 694
Arbeiten mit Oracle Solaris IP Filter-Regellisten ... 695
Verwalten der Paketfilter-Regellisten für Oracle Solaris IP Filter ... 696
Verwalten der NAT-Regeln für Oracle Solaris IP Filter ... 703
Verwalten der Adresspools für Oracle Solaris IP Filter ... 705
Anzeigen von Statistiken und Informationen zu Oracle Solaris IP Filter ... 707
▼ So zeigen Sie die Statustabellen für Oracle Solaris IP Filter an ... 707
▼ So zeigen Sie die Statusstatistiken für Oracle Solaris IP Filter an ... 708
▼ So zeigen Sie die NAT-Statistiken für Oracle Solaris IP Filter an ... 709
▼ So zeigen Sie die Adresspool-Statistiken für Oracle Solaris IP Filter an ... 709
Arbeiten mit Protokolldateien für Oracle Solaris IP Filter ... 710
▼ So richten Sie eine Protokolldatei für Oracle Solaris IP Filter ein ... 710
▼ So zeigen Sie Oracle Solaris IP Filter-Protokolldateien an ... 711
▼ So leeren Sie die Paketprotokolldatei ... 713
▼ So speichern Sie protokollierte Pakete in einer Datei ... 713
Erstellen und Bearbeiten von Konfigurationsdateien für Oracle Solaris IP Filter ... 714
▼ So erstellen Sie eine Konfigurationsdatei für Oracle Solaris IP Filter ... 715
Beispiel für Oracle Solaris IP Filter-Konfigurationsdateien ... 716

Teil V Mobile IP ... 721

27 Mobile IP (Übersicht) ... 723
Neuerungen bei Mobile IP ... 723
Einführung in Mobile IP ... 724
Mobile IP-Funktionseinheiten ... 726
Arbeitsweise von Mobile IP ... 726
Agent-Erkennung ... 729
Agent Advertisement ... 729

Agent Solicitation ... 730
Care-of-Adressen ... 730
Mobile IP mit Rücktunnel ... 731
Eingeschränkte Unterstützung für private Adressen ... 732
Mobile IP-Registrierung ... 733
Network Access Identifier (NAI) ... 736
Mobile IP-Nachrichtenauthentifizierung ... 736
Registrierungsanforderung eines mobilen Knotens ... 736
Antwort auf eine Registrierungsanforderung ... 737
Überlegungen zum Foreign-Agent ... 737
Überlegungen zum Home-Agent ... 737
Dynamische Home-Agent-Erkennung ... 738
Routen von Datagrammen von und an mobile Knoten ... 738
Methoden zur Einkapselung ... 738
Routing von Unicast Datagrammen ... 739
Broadcast-Datagramme ... 739
Routing von Multicast-Datagrammen ... 740
Sicherheitsbetrachtungen für Mobile IP ... 741

28 Verwalten von Mobile IP (Aufgaben) ... 743
Erstellen einer Mobile IP-Konfigurationsdatei (Übersicht der Schritte) ... 743
Erstellen einer Mobile IP-Konfigurationsdatei ... 744
▼ So planen Sie für Mobile IP ... 744
▼ So erstellen Sie eine Mobile IP-Konfigurationsdatei ... 745
▼ So konfigurieren Sie den Abschnitt `General` ... 746
▼ So konfigurieren Sie den Abschnitt `Advertisements` ... 746
▼ So konfigurieren Sie den Abschnitt `GlobalSecurityParameters` ... 746
▼ So konfigurieren Sie den Abschnitt `Pool` ... 747
▼ So konfigurieren Sie den Abschnitt `SPI` ... 747
▼ So konfigurieren Sie den Abschnitt `Address` ... 747
Ändern der Mobile IP-Konfigurationsdatei (Übersicht der Schritte) ... 748
Ändern einer Mobile IP-Konfigurationsdatei ... 749
▼ So ändern Sie den Abschnitt `General` ... 749
▼ So ändern Sie den Abschnitt `Advertisements` ... 750
▼ So ändern Sie den Abschnitt `GlobalSecurityParameters` ... 751

▼ So ändern Sie den Abschnitt `Pool` 751
▼ So ändern Sie den Abschnitt `SPI` 752
▼ So ändern Sie den Abschnitt `Address` 752
▼ So fügen einer Konfigurationsdatei Parameter hinzu bzw. löschen Parameter 753
▼ So zeigen Sie die aktuellen Parameterwerte in der Konfigurationsdatei an 754
Anzeigen des Mobility-Agent-Status 756
▼ So zeigen Sie den Mobility-Agent-Status an 756
Anzeigen der Mobility-Routen auf einem Foreign-Agent 757
▼ So zeigen Sie die Mobility-Routen auf einem Foreign-Agent an 757

29 Mobile IP-Dateien und Befehle (Referenz) 759
Overview of the Solaris Mobile IP Implementation 759
Mobile IP-Konfigurationsdatei 760
Format der Konfigurationsdatei 761
Beispiele für die Konfigurationsdatei 761
Abschnitte und Label in der Konfigurationsdatei 764
Konfiguration des Mobility IP-Agent 773
Status des Mobile IP Mobility-Agent 774
Informationen zum Mobile IP-Status 775
`netstat`-Erweiterungen für Mobile IP 775
`snoop`-Erweiterungen für Mobile IP 776

Teil VI IPMP 777

30 Einführung in IPMP (Übersicht) 779
Gründe für IPMP 779
Oracle Solaris IPMP-Komponenten 780
IPMP-Terminologie und Konzepte 781
Allgemeine Anforderungen von IPMP 783
IPMP-Adressierung 784
Datenadressen 784
Testadressen 784
Verwenden der Testadressen durch Anwendungen verhindern 786
IPMP-Schnittstellenkonfigurationen 787

Standby-Schnittstellen in einer IPMP-Gruppe 787
Allgemeine IPMP-Schnittstellenkonfigurationen 788
IPMP-Funktionen zur Ausfall- und Reparaturerkennung 789
Stichproben-basierte Ausfallerkennung 789
Stichproben-basierte Ausfallerkennung 790
Ausfall einer Gruppe 791
Erkennen der Reparatur physikalischer Schnittstellen 791
Vorgänge während eines Schnittstellen-Failover 791
IPMP und Dynamische Rekonfiguration 793
Anschließen von NICs 794
Trennen von NICs 794
Wiederanschließen von NICs 795
Bei einem Systemstart fehlende NICs 795

31 Verwaltung von IPMP (Aufgaben) 797
Konfiguration von IPMP (Übersicht der Schritte) 797
Konfiguration und Verwaltung von IPMP-Gruppen (Übersicht der Schritte) 798
Verwalten von IPMP auf Schnittstellen, die DR unterstützen (Übersicht der Schritte) 799
Konfiguration von IPMP-Gruppen 799
Planung für eine IPMP-Gruppe 799
Konfiguration von IPMP-Gruppen 801
Konfiguration von IPMP-Gruppen mit einer physikalischen Schnittstelle 810
Verwalten von IPMP-Gruppen 812
▼ So zeigen Sie die IPMP-Gruppenmitgliedschaft einer Schnittstelle an 812
▼ So fügen Sie eine Schnittstelle zu einer IPMP-Gruppe hinzu 813
▼ So entfernen Sie eine Schnittstelle aus einer IPMP-Gruppe 814
▼ So verschieben Sie eine Schnittstelle von einer IPMP-Gruppe in eine andere 815
Ersetzen einer ausgefallenen physikalischen Schnittstelle auf Systemen, die DR unterstützen 815
▼ So entfernen Sie eine ausgefallene physikalische Schnittstelle (DR-Detach) 816
▼ So ersetzen Sie eine ausgefallene physikalische Schnittstelle (DR-Attach) 817
Wiederherstellung einer physikalischen Schnittstelle, die beim Systemstart nicht vorhanden war 818
▼ So stellen Sie eine physikalische Schnittstelle wieder her, die beim Systemstart nicht vorhanden war 818
Ändern von IPMP-Konfigurationen 820

▼ So konfigurieren Sie die `/etc/default/mpathd`-Datei 821

Teil VII IP Quality of Service (IPQoS) 823

32 Einführung in IPQoS (Übersicht) 825
Grundlagen von IPQoS 825
Was sind Differentiated Services? 825
Funktionen von IPQoS 826
Weitere Informationen zur Theorie und Praxis von Quality-of-Service 826
Bereitstellen von Quality of Service mit IPQoS 828
Umsetzen von Service-Level Agreements 828
Sicherstellen des Quality of Service für eine einzelne Organisation 828
Einführung in die Quality of Service-Richtlinie 828
Verbessern der Netzwerkeffizienz mit IPQoS 829
So wirkt sich die Bandbreite auf den Netzwerkverkehr aus 830
Verwenden von Serviceklassen zum Priorisieren von Verkehr 830
Differentiated Services-Modell 831
Classifier (`ipgpc`) – Übersicht 831
Meter (`tokenmt` und `tswtclmt`) – Übersicht 833
Marker (`dscpmk` und `dlcosmk`) – Übersicht 833
Flow Accounting (`flowacct`) – Übersicht 834
So durchläuft ein Verkehrswert die IPQoS-Module 834
Verkehrsweiterleitung in einem IPQoS-konformen Netzwerk 836
DS Codepoint 836
Per-Hop-Behaviors 836

33 Planen eines IPQoS-konformen Netzwerks (Aufgaben) 841
Planen einer allgemeinen IPQoS-Konfiguration (Übersicht der Schritte) 841
Planen der Diffserv-Netzwerktopologie 842
Hardware-Strategien für das Diffserv-Netzwerk 842
IPQoS-Netzwerktopologien 843
Planen der Quality of Service-Richtlinie 845
Hilfen bei der Planung einer QoS-Richtlinie 845
Planen einer QoS-Richtlinie (Übersicht der Schritte) 846

▼ So bereiten Sie ein Netzwerk für IPQoS vor 847
▼ So definieren Sie die Klassen für Ihre QoS-Richtlinie 848
Definieren von Filtern 850
▼ So definieren Sie Filter in der QoS-Richtlinie 851
▼ So planen Sie die Verkehrssteuerung 852
▼ So planen Sie das Weiterleitungsverhalten 855
▼ So planen Sie das Flow Accounting 858
Einführung in das IPQoS-Konfigurationsbeispiel 859
IPQoS-Topologie 859

34 Erstellen der IPQoS-Konfigurationsdatei (Aufgaben) 863
Definieren einer QoS-Richtlinie in der IPQoS-Konfigurationsdatei (Übersicht der Schritte) 863
Tools zum Erstellen einer QoS-Richtlinie 865
Allgemeine IPQoS-Konfigurationsdatei 865
Erstellen von IPQoS-Konfigurationsdateien für Webserver 866
▼ So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen . 868
▼ So definieren Sie Filter in der IPQoS-Konfigurationsdatei 870
▼ So definieren Sie das Weiterleiten von Datenverkehr in der IPQoS-Konfigurationsdatei 872
▼ So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei 875
▼ So erstellen Sie eine IPQoS-Konfigurationsdatei für einen Beste Leistung-Webserver 877
Erstellen einer IPQoS-Konfigurationsdateien für einen Anwendungsserver 880
▼ So konfigurieren Sie die IPQoS-Konfigurationsdatei für einen Anwendungsserver 882
▼ So konfigurieren Sie die Weiterleitung von Datenverkehr für Anwendungen in der IPQoS-Konfigurationsdatei 884
▼ So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei 887
Bereitstellen von Differentiated Services auf einem Router 890
▼ So konfigurieren Sie einen Router in einem IPQoS-konformen Netzwerk 890

35 Starten und Verwalten des IPQoS (Aufgaben) 893
Verwalten des IPQoS (Übersicht der Schritte) 893
Übernehmen einer IPQoS-Konfiguration 894
▼ So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module 894
▼ So stellen Sie sicher, dass die IPQoS-Konfiguration bei jedem Systemstart übernommen wird 895
Aktivieren von `syslog` zum Protokollieren von IPQoS-Nachrichten 896

▼ So aktivieren Sie die Protokollierung von IPQoS-Nachrichten während des Bootens 896
Fehlerbehebung mit IPQoS-Fehlermeldungen 897

36 Verwenden von Flow Accounting und Erfassen von Statistiken (Aufgaben) 901
Einrichten des Flow Accounting (Übersicht der Schritte) 901
Aufzeichnen von Informationen zu Verkehrswerten 902
▼ So erstellen Sie eineDatei für die Flow Accounting-Daten 902
Erfassen statistischer Informationen 904

37 IPQoS im Detail (Referenz) 907
IPQoS-Architektur und das Diffserv-Modell 907
Classifier-Modul 907
Metermodul 910
Markermodul 913
`flowacct`-Modul 917
IPQoS-Konfigurationsdatei 920
`action`-Anweisung 921
Definition der Module 922
`class`-Klausel 923
`filter`-Klausel 923
`params`-Klausel 924
`ipqosconf`-Konfigurationsprogramm 924

Glossar 925

Index 937

Vorwort

Systemverwaltungshandbuch: IP Services ist Teil eines neunbändigen Dokumentationssatzes, der zahlreiche wichtige Informationen zur Verwaltung des Oracle Solaris-Betriebssystems enthält. Es wird davon ausgegangen, dass Oracle Solaris 10 bereits installiert ist. Sie sollten in der Lage sein, Ihr Netzwerk oder die für Ihr Netzwerk erforderliche Netzwerksoftware zu konfigurieren. Oracle Solaris 10 ist Teil der Oracle Solaris-Produktfamilie, zu der auch das Java Desktop System gehört. Oracle Solaris ist kompatibel mit dem Betriebssystem System V, Release 4 von AT&T.

Hinweis – Diese Oracle Solaris-Version unterstützt Systeme auf der Basis der Prozessorarchitekturen SPARC und x86. Die unterstützten Systeme werden unter Solaris OS: Hardware Compatibility Lists (`http://www.sun.com/bigadmin/hcl`) aufgeführt. Eventuelle Implementierungsunterschiede zwischen den Plattformtypen sind in diesem Dokument angegeben.

In diesem Dokument bedeuten x86-bezogene Begriffe Folgendes:

- „x86” bezeichnet die weitere Familie an Produkten, die mit 64-Bit- und 32-Bit-x86-Architekturen kompatibel sind.
- "x64" bezieht sich insbesondere auf mit 32-Bit-x86-Architekturen kompatible CPUs.
- „32-Bit x86“ weist auf spezifische, für 32-Bit-Systeme geltende Informationen zu x86-basierten Systemen hin.

Die unterstützten Systeme können Sie der *Solaris OS: Hardware-Kompatibilitätsliste* entnehmen.

Zielgruppe dieses Handbuchs

Dieses Buch richtet sich an Systemadministratoren, die für die Verwaltung von Systemen verantwortlich sind, auf denen Oracle Solaris ausgeführt wird und die an ein Netzwerk angeschlossen sind. Um die Informationen in diesem Buch korrekt umsetzen zu können, sollten Sie über mindestens zwei Jahre Erfahrung in der Verwaltung von UNIX-Systemen verfügen. Die Teilnahme an Schulungen zur Verwaltung von UNIX-Systemen wird empfohlen.

Organisation der Systemverwaltungshandbücher

Hier finden Sie eine Liste der Themen, die in den Systemverwaltungshandbüchern behandelt werden.

Buchtitel	Themen
System Administration Guide: Basic Administration	Benutzerkonten und Gruppen, Server- und Clientunterstützung, Herunterfahren und Booten eines Systems, Verwalten der Services
System Administration Guide: Advanced Administration	Terminale und Modems, Systemressourcen (Datenträgerkontingente, Accounting und Crontabs), Systemprozesse und Beheben von Problemen mit der Oracle Solaris-Software
System Administration Guide: Devices and File Systems	Wechselmedien, Festplatten und Geräte, Dateisysteme und Sichern und Wiederherstellen von Daten
Systemverwaltungshandbuch: IP Services	TCP/IP-Netzwerkverwaltung, IPv4- und IPv6-Adressverwaltung, DHCP, IPsec, IKE, Oracle Solaris IP Filter, Mobile IP, IP-Netzwerk-Multipathing (IPMP) und IPQoS
System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)	DNS-, NIS- und LDAP-Benennungs- und Verzeichnisservices, einschließlich Übergang von NIS zu LDAP und Übergang von NIS+ zu LDAP
System Administration Guide: Naming and Directory Services (NIS+)	NIS+ Benennungs- und Verzeichnisservices
System Administration Guide: Network Services	Webcache-Server, zeitorientierte Services, Netzwerk-Dateisysteme (NFS und Autofs), Mail, SLP und PPP
System Administration Guide: Printing	Druckthemen und -aufgaben, wie Sie mithilfe von Services, Tools, Protokollen und Technologien Druckdienste und Drucker einrichten und verwalten
System Administration Guide: Security Services	Auditing, Geräteverwaltung, Dateisicherheit, BART, Kerberos-Services, PAM, Solaris Cryptographic Framework, Berechtigungen, RBAC, SASL und Solaris Secure Shell
Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones	Projekte und Aufgaben im Rahmen der Ressourcenverwaltung, Extended Accounting, Resource Controls, Fair Share Scheduler (FSS), Steuerung des physischen Arbeitsspeichers mithilfe des Resource Capping Daemon (rcapd) und Resource Pools; Virtualisierung mithilfe der Softwarepartitionierungstechnologie Solaris Zones und `lx`-Branded Zones

Buchtitel	Themen
Oracle Solaris ZFS-Administrationshandbuch	ZFS-Speicherpool und Dateisystemerstellung und -verwaltung, Momentaufnahmen, Klone, Backups, verwenden von Zugriffssteuerlisten (Access Control Lists/ACLs) zum Schutz von ZFS-Dateien, verwenden von ZFS auf einem Solaris-System mit installierten Zonen, emulierte Datenträger und Problembehandlung und Datenwiederherstellung
Oracle Solaris Trusted Extensions Administrator's Procedures	Systemadministration, die nur für die Trusted Extensions-Funktion von Oracle Solaris gilt
Oracle Solaris Trusted Extensions Configuration Guide	Ab Version Solaris 10 5/08: Hier wird beschrieben, wie Sie die Trusted Extensions-Funktion von Oracle Solaris planen, aktivieren und die Erstkonfiguration durchführen.

Verwandte Dokumentation

In diesem Handbuch werden Informationen aus den folgenden Publikationen verwendet.

- Stevens, W. Richard. *TCP/IP Illustrated, Volume 1, The Protocols*. Addison Wesley, 1994.
- Hunt Craig.*TCP/IP Network Administration, 3rd Edition*. O'Reilly, 2002.
- Perkins, Charles E. *Mobile IP Design Principles and Practices* . Massachusetts, 1998, Addison-Wesley Publishing Company.
- Solomon, James D. *Mobile IP: The Internet Unplugged*. New Jersey, 1998, Prentice-Hall, Inc.
- Ferguson, Paul and Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

Themenverwandte Websites von Fremdanbietern

In dieser Dokumentation wird auf URLs von Fremdanbietern verwiesen, auf denen zusätzliche relevante Informationen zur Verfügung gestellt werden.

Hinweis – Sun ist nicht für die Verfügbarkeit der in diesem Dokument erwähnten Websites anderer Hersteller verantwortlich. Sun haftet nicht für den Inhalt oder Werbung auf diesen Websites oder für die auf diesen Websites angebotenen Produkte und Materialien. Sun übernimmt keine Verantwortung oder Haftung für tatsächliche oder angebliche Schäden oder Verluste, die im Zusammenhang mit den auf diesen Websites angebotenen Informationen, Waren oder Dienstleistungen entstanden sind.

Oracle Solaris IP Filter ist von der Open Source IP Filter-Software abgeleitet. Der Standardpfad zu Anzeige der Lizenzbedingungen, Attribution und der Hinweise zum Copyright für IP Filter

lautet /usr/lib/ipf/IPFILTER.LICENCE. Falls Oracle Solaris nicht unter dem Standardpfad installiert wurde, ändern Sie den angegebenen Pfad so, dass Sie auf die Datei im Installationsverzeichnis zugreifen können.

Dokumentation, Support und Schulung

Weitere Ressourcen finden Sie auf der folgenden Website:

- Dokumentation (http://docs.sun.com)
- Support (http://www.oracle.com/us/support/systems/index.html)
- Schulung (http://education.oracle.com) – Klicken Sie in der linken Navigationsleiste auf den Sun-Link.

Ihre Meinung ist gefragt

Oracle ist an Ihrer Meinung und an Ihren Anregungen zur Qualität und zum Nutzen der vorliegenden Dokumentation interessiert. Wenn Sie Fehler finden oder Verbesserungsvorschläge haben, gehen Sie zu http://docs.sun.com, und klicken Sie dann auf "Feedback". Geben Sie den Titel und die Teilenummer der Dokumentation und wenn möglich das Kapitel, den Abschnitt und die Seitennummer an. Teilen Sie uns bitte mit, ob Sie eine Antwort wünschen.

Das Oracle-Technologienetzwerk (http://www.oracle.com/technetwork/index.html) bietet zahlreiche Ressourcen für Oracle-Software:

- Sie können technische Probleme und Lösungen in den Diskussionsforen (http://forums.oracle.com) diskutieren.
- Nutzen Sie praktische schrittweise Lernprogramme mit Oracle By Example (http://www.oracle.com/technology/obe/start/index.html).
- Laden Sie den Sample Code herunter (http://www.oracle.com/technology/sample_code/index.html).

Typografische Konventionen

In der folgenden Tabelle sind die in diesem Handbuch verwendeten typografischen Konventionen aufgeführt.

TABELLE P–1 Typografische Konventionen

Schriftart	Bedeutung	Beispiel
`AaBbCc123`	Die Namen von Befehlen, Dateien, Verzeichnissen sowie Bildschirmausgabe.	Bearbeiten Sie Ihre `.login`-Datei. Verwenden Sie `ls -a`, um eine Liste aller Dateien zu erhalten. `system% Sie haben eine neue Nachricht.`
`AaBbCc123`	Von Ihnen eingegebene Zeichen (im Gegensatz zu auf dem Bildschirm angezeigten Zeichen)	`Computername%` **`su`** `Passwort:`
aabbcc123	Platzhalter: durch einen tatsächlichen Namen oder Wert zu ersetzen	Der Befehl zum Entfernen einer Datei lautet `rm` *Dateiname*.
AaBbCc123	Buchtitel, neue Ausdrücke; hervorgehobene Begriffe	Lesen Sie hierzu Kapitel 6 im *Benutzerhandbuch*. Ein *Cache* ist eine lokal gespeicherte Kopie. Diese Datei *nicht* speichern. **Hinweis:** Einige hervorgehobene Begriffe werden online fett dargestellt.

Shell-Eingabeaufforderungen in Befehlsbeispielen

Die folgende Tabelle zeigt die Standard-Systemeingabeaufforderung von UNIX und die Superuser-Eingabeaufforderung für Shells, die in Oracle Solaris enthalten sind. Beachten Sie, dass die in den Beispielen gezeigte Standard-Systemeingabeaufforderung je nach Oracle Solaris-Version unterschiedlich ist.

TABELLE P–2 Shell-Eingabeaufforderungen

Shell	Eingabeaufforderung
Bash-Shell, Korn-Shell und Bourne-Shell	`$`
Bash-Shell, Korn-Shell und Bourne-Shell für Superuser	`#`
C-Shell	`system%`
C-Shell für Superuser	`system#`

TEIL I

Einführung in die Systemverwaltung: IP Services

Dieser Teil enthält eine Einführung in die TCP/IP-Protokollfamilie sowie deren Implementierung in Oracle Solaris.

KAPITEL 1

Oracle Solaris TCP/IP-Protokollfamilie (Übersicht)

Dieses Kapitel enthält eine Einführung in die Umsetzung der Netzwerk-Protokollfamilie TCP/IP in Oracle Solaris. Es richtet sich an System- und Netzwerkadministratoren, die nicht mit den Grundlagen der TCP/IP-Konzepte vertraut sind. Im restlichen Teil dieses Handbuchs wird davon ausgegangen, dass Sie mit diesen Konzepten vertraut sind.

Dieses Kapitel enthält die folgenden Informationen:

- „Einführung in die TCP/IP-Protokollfamilie" auf Seite 37
- „So verarbeiten TCP/IP-Protokolle die Datenkommunikation" auf Seite 45
- „Weitere Informationen zu TCP/IP und dem Internet" auf Seite 49

Neuheiten in dieser Version

Ab Solaris 10 5/08 wurde die Mobile IP-Funktion entfernt. Mobile IP ist in Solaris 10 OS 8/07 und früheren Versionen verfügbar.

Einführung in die TCP/IP-Protokollfamilie

Dieser Abschnitt enthält eine umfassende Einführung in die in TCP/IP enthaltenen Protokolle. Obwohl diese Informationen nur als Hintergrundwissen dienen, sollten Sie die Namen der Protokolle kennen. Darüber hinaus sollten Sie wissen, was jedes einzelne Protokoll zu leisten hat.

„TCP/IP" ist ein Akronym, das häufig für den Satz der Netzwerkprotokolle verwendet wird, aus denen sich die *Internet Protocol-Familie* zusammensetzt. Vielfach wird der Begriff „Internet" verwendet, um sowohl die Protokollfamilie als auch das globale WAN-Netzwerk zu beschreiben. In diesem Buch bezieht sich „TCP/IP" ausschließlich auf die Internet Protocol-Familie. „Internet" bezieht sich auf das Weitverkehrsnetz (WAN) und die Einrichtungen, die das Internet überwachen.

Um Ihr TCP/IP-Netzwerk mit anderen Netzwerken zu vernetzen, müssen Sie eine einmalige IP-Adresse für Ihr Netzwerk beziehen. Zum Zeitpunkt der Erstellung dieser Publikation beziehen Sie diese Adresse von einem Internet Service Provider (ISP).

Wenn Hosts in Ihrem Netzwerk am Internet Domain-Namen-System (DNS) teilnehmen sollen, müssen Sie einen einmaligen Domänennamen beziehen und registrieren. Die Registrierung der Domänennamen wird von InterNIC über eine Gruppe von weltweiten Datenbanken koordiniert. Weitere Informationen zum DNS finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

Protokollschichten und das Open Systems Interconnection-Modell

Die meisten Netzwerk-Protokollfamilien sind in mehreren Schichten unterteilt, die in ihrer Gesamtheit auch als *Protokollstapel* bezeichnet werden. Jede Schicht dient einem bestimmten Zweck. Jede Schicht ist sowohl auf dem sendenden als auch auf dem empfangenden System vorhanden. Eine bestimmte Schicht eines Systems sendet bzw. empfängt genau das gleiche Objekt, das der *Peer-Prozess* eines anderen Systems gesendet bzw. empfangen hat. Diese Aktivitäten treten unabhängig von anderen Aktivitäten in den Schichten über bzw. unter der betrachteten Schicht auf. Grundsätzlich agiert jede Schicht eines Systems unabhängig von den anderen Schichten auf dem gleichen System. Jede Schicht agiert parallel mit der gleichen Schicht auf anderen Systemen.

OSI-Referenzmodell

Die meisten Netzwerk-Protokollfamilien sind in Schichten aufgebaut. Die International Organization for Standardization (ISO) hat das Open Systems Interconnection (OSI)-Referenzmodell entworfen, in dem strukturierte Schichten verwendet werden. Das OSI-Modell beschreibt eine Struktur von sieben Schichten für Netzwerkaktivitäten. Jeder Schicht ist mindestens ein Protokoll zugeordnet. Die Schichten stellen die Datenübertragungsvorgänge dar, die allen Datenübertragungsarten zwischen kooperierenden Netzwerken gemein sind.

Das OSI-Modell führt die Protokollschichten von der obersten (Schicht 7) zur untersten (Schicht 1) auf. Dieses Modell wird in der folgenden Tabelle gezeigt.

TABELLE 1–1 OSI-Referenzmodell

Schichtnr.	Name	Beschreibung
7	Anwendung	Umfasst die standardmäßigen Kommunikationsservices und Anwendungen, mit denen der Benutzer arbeitet.
6	Darstellung	Stellt sicher, dass Informationen so an das empfangende System geliefert werden, dass sie vom System verstanden werden.

TABELLE 1–1 OSI-Referenzmodell *(Fortsetzung)*

Schichtnr.	Name	Beschreibung
5	Sitzung	Verwaltet die Verbindungen und Abschlüsse zwischen kooperierenden Systemen.
4	Transport	Verwaltet die Datenübertragung. Stellt darüber hinaus sicher, dass die empfangenen Daten mit den gesendeten Daten übereinstimmen.
3	Vermittlung	Verwaltet die Datenadressierung und die Übermittlung zwischen Netzwerken.
2	Sicherung	Verarbeitet die Übertragung der Daten über die Netzwerkmedien.
1	Bitübertragung	Definiert die Eigenschaften der Netzwerkhardware.

Das OSI-Modell definiert konzeptuelle Vorgänge, die nicht an eine bestimmte Netzwerkprotokollfamilie gebunden sind. Beispielsweise implementiert die OSI-Netzwerk-Protokollfamilie alle sieben Schichten des OSI-Modells. TCP/IP verwendet ebenfalls einige Schichten des OSI-Modells, und fasst andere Schichten zusammen. Andere Netzwerkprotokolle, z. B. SNA, verwenden eine zusätzliche achte Schicht.

Modell der TCP/IP-Protokollarchitektur

Das OSI-Modell beschreibt idealisierte Netzwerkverbindungen mit einer Protokollfamilie. TCP/IP entspricht in diesem Modell nur zum Teil. Es verbindet z. B. mehrere OSI-Schichten zu einer Schicht oder verwendet andere Schichten gar nicht. In der folgenden Tabelle sind die Schichten der Implementierung von TCP/IP in Oracle Solaris aufgeführt. In der folgenden Tabelle sind die Schichten von der obersten Schicht (Anwendung) zur untersten Schicht (Bitübertragung) aufgeführt.

TABELLE 1–2 TCP/IP-Protokollstapel

OSI Ref. Schichtnr.	Entsprechende OSI-Schicht	TCP/IP-Schicht	TCP/IP-Protokollbeispiele
5,6,7	Anwendung, Sitzung, Darstellung	Anwendung	NFS, NIS, DNS, LDAP, `telnet`, `ftp`, `rlogin`, `rsh`, `rcp`, RIP, RDISC, SNMP und andere
4	Transport	Transport	TCP, UDP, SCTP
3	Vermittlung	Internet	IPv4, IPv6, ARP, ICMP
2	Sicherung	Sicherung	PPP, IEEE 802.2
1	Bitübertragung	Bitübertragung	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI und andere

Die Tabelle zeigt die TCP/IP-Protokollschichten und deren Entsprechungen im OSI-Modell. Darüber hinaus sind Beispiele der Protokolle aufgeführt, die auf jeder Schicht im TCP/IP-Protokollstapel verfügbar sind. Jedes an einem Datenaustausch beteiligte System führt eine einmalige Implementierung des Protokollstapels aus.

Bitübertragungsschicht

Die *Bitübertragungsschicht* legt die Eigenschaften der für das Netzwerk verwendeten Hardware fest. Beispielsweise bestimmt die Bitübertragungsschicht die physikalischen Eigenschaften der Kommunikationsmedien. Die Bitübertragungsschicht im TCP/IP-Protokoll beschreibt Hardwarestandards wie IEEE 802.3, die Spezifikationen der Ethernet-Netzwerkmedien und RS-232, die Spezifikationen für standardmäßige Pin-Stecker.

Sicherungsschicht

Die *Sicherungsschicht* identifiziert den Netzwerkprotokolltyp des Pakets, in diesem Fall TCP/IP. Darüber hinaus bietet die Sicherungsschicht eine Fehlerkontrolle und Daten-Framing. Beispiele für Protokolle in der Sicherungsschicht sind Ethernet IEEE 802.2 Framing und Point-to-Point Protocol (PPP)-Framing.

Vermittlungsschicht

Die Vermittlungsschicht, die auch als *Internetschicht* oder *IP-Schicht* bezeichnet wird, akzeptiert Pakete und gibt sie an das Netzwerk weiter. Diese Schicht umfasst das mächtige Internet Protocol (IP), das Address Resolution Protocol (ARP) und das Internet Control Message Protocol (ICMP).

IP-Protokoll

Das IP-Protokoll und die dazugehörigen Routing-Protokolle sind wahrscheinlich die wichtigsten Protokolle der gesamten TCP/IP-Protokollfamilie. Das IP-Protokoll ist für Folgendes verantwortlich:

- **IP-Adressierung** – die IP-Adressierungskonventionen sind Teil des IP-Protokolls. „Erstellen eines IPv4-Adressierungsschemas“ auf Seite 61 enthält eine Einführung in die IPv4-Adressierung, „Einführung in die IPv6-Adressierung“ auf Seite 78 in die IPv6-Adressierung.
- **Host zu Host-Kommunikation** – Das IP-Protokoll bestimmt den Pfad, den ein Paket nehmen muss, anhand der IP-Adresse des empfangenden Systems.
- **Paket-Formatierung** – Das IP-Protokoll setzt Datenpakete zu Einheiten zusammen, die als *Datagramme* bezeichnet werden. Datagramme sind ausführlich unter „Internetschicht: Vorbereitung der Pakete für die Zustellung“ auf Seite 48 beschrieben.

- **Fragmentierung** – Falls ein Paket zu groß für die Übertragung über das Netzwerkmedium ist, schlüsselt das IP-Protokoll das Paket auf dem sendenden System in kleinere Fragmente auf. Das IP-Protokoll auf dem empfangenden System setzt die Fragmente dann wieder zum Originalpaket zusammen.

Oracle Solaris unterstützt die Adressierungsformate IPv4 und IPv6, die beide in diesem Handbuch beschrieben werden. Um Missverständnissen vorzubeugen, wird eine der folgenden Konventionen bei der Bezeichnung der Internet Protocol-Versionen verwendet:

- Wenn der Begriff „IP" in einer Beschreibung verwendet wird, gilt die Beschreibung für IPv4 und IPv6.
- Wenn der Begriff „IPv4" in einer Beschreibung verwendet wird, geht die Beschreibung nur für IPv4.
- Wenn der Begriff „IPv6" in einer Beschreibung verwendet wird, geht die Beschreibung nur für IPv6.

ARP-Protokoll

Das Address Resolution Protocol (ARP) befindet sich zwischen der Sicherungs- und der Vermittlungsschicht. ARP unterstützt das IP-Protokoll dabei, Datagramme an das richtige empfangende System zu leiten, indem es Ethernet-Adressen (mit einer Länge von 48 Bit) zu bekannten IP-Adressen (mit einer Länge von 32 Bit) zuordnet.

ICMP-Protokoll

Das Internet Control Message Protocol (ICMP) erkennt und meldet Fehlerzustände im Netzwerk. ICMP meldet Folgendes:

- **Verlorene Pakete** – Pakete, die zu schnell ankommen, um verarbeitet zu werden
- **Konnektivitätsfehler** – Ein Zielsystem kann nicht erreicht werden
- **Umleitung** – Das Umleiten eines sendenden Systems, so dass es einen anderen Router verwendet

Kapitel 8, „Verwaltung eines TCP/IP-Netzwerks (Aufgaben)" enthält weitere Informationen zu den Oracle Solaris-Befehlen, die das ICMP-Protokoll zur Fehlererkennung verwenden.

Transportschicht

Die *Transportschicht* im TCP/IP-Protokoll stellt sicher, dass Pakete nacheinander und fehlerfrei eintreffen, indem es Bestätigungen für den Datenempfang sendet und verlorene Pakete erneut überträgt. Diese Kommunikationsart wird als *durchgehende (End-to-End)* Kommunikation bezeichnet. Transportschichtprotokolle auf dieser Stufe sind Transmission Control Protocol (TCP), User Datagram Protocol (UDP) und Stream Control Transmission Protocol (SCTP). TCP und SCTP stellen zuverlässige End-to-End-Services bereit. UDP stellt unzuverlässigen Datagramm-Service bereit.

TCP-Protokoll

TCP sorgt dafür, dass Anwendungen so miteinander kommunizieren können, als wären sie über einen Schaltkreis fest miteinander verbunden. TCP sendet Daten zeichenweise anstatt in diskreten Paketen. Die Übertragung setzt sich aus Folgendem zusammen:

- Startpunkt, der die Verbindung öffnet.
- Gesamte Übertragung in Byte-Reihenfolge.
- Endpunkt, der die Verbindung schließt.

TCP fügt den übertragenen Daten einen Header hinzu. Dieser Header enthält zahlreiche Parameter, die Prozesse auf dem sendenden System dabei unterstützen, die Verbindung mit den Peer-Prozessen auf dem empfangenden System herzustellen.

TCP bestätigt, dass ein Paket sein Ziel erreicht hat, indem es eine End-to-End-Verbindung zwischen dem sendenden und dem empfangenden Host herstellt. Daher wird TCP als ein „zuverlässiges, verbindungsorientiertes" Protokoll bezeichnet.

SCTP-Protokoll

SCTP ist ein zuverlässiges, verbindungsorientiertes Transportschichtprotokoll, das Anwendungen die gleichen Services wie das TCP-Protokoll bereitstellt. Darüber hinaus kann das SCTP-Protokoll auch Verbindungen zwischen Systemen unterstützen, die über mehrere Adressen verfügen (*Multihomed Systeme*). Die SCTP-Verbindung zwischen dem sendenden und dem empfangenden System wird als *Assoziation* bezeichnet. Daten in der Assoziation sind in Datenblöcke aufgeteilt. Da das SCTP-Protokoll multihoming unterstützt, müssen bestimmte Anwendungen (insbesondere Anwendungen für die Telekommunikationsindustrie) über SCTP anstatt TCP ausgeführt werden.

UDP-Protokoll

UDP bietet einen Zustellungsservice für Datagramme. UDP überprüft keine Verbindungen zwischen sendenden und empfangenden Hosts. Da UDP keine Prozesse zum Herstellen und Überprüfen von Verbindungen ausführt, verwenden Anwendungen, die nur geringe Datenmengen senden, das UDP-Protokoll.

Anwendungsschicht

Die *Anwendungsschicht* definiert standardmäßige Internetservices und Netzwerkanwendungen, die jeder verwenden kann. Diese Services arbeiten zum Senden und Empfangen von Daten mit der Transportschicht zusammen. Auf der Anwendungsschicht existieren verschiedene Protokolle. Die folgende Liste zeigt Beispiele für Protokolle der Anwendungsschicht:

- Standardmäßige TCP/IP-Services wie z. B. `ftp`, `tftp` und `telnet`-Befehle
- UNIX „r"-Befehle, z. B. `rlogin` und `rsh`

- Namen-Services, z. B. NIS und Domain-Namen-Service (DNS)
- Verzeichnisservices (LDAP)
- Dateiservices, z. B. der NFS-Service
- Simple Network Management Protocol (SNMP), das eine Netzwerkverwaltung ermöglicht
- Die Routing-Protokolle Router Discovery Server Protocol (RDISC) und Routing Information Protocol (RIP)

Standardmäßige TCP/IP-Services

- **FTP und Anonymous FTP** – Das File Transfer Protocol (FTP) überträgt Dateien von und an ein Remote-Netzwerk. Das Protokoll umfasst den Befehl `ftp` und den Daemon `in.ftpd.` Mit FTP kann ein Benutzer den Namen eines Remote-Host und Optionen des Dateiübertragungsbefehls an der Befehlszeile des lokalen Hosts eingeben. Der `in.ftpd`-Daemon auf dem Remote-Host verarbeitet daraufhin die Anforderungen vom lokalen Host. Im Gegensatz zu `rcp` arbeitet `ftp` auch dann korrekt, wenn der Remote-Computer kein UNIX-basiertes Betriebssystem ausführt. Zum Herstellen einer `ftp`-Verbindung muss sich ein Benutzer beim Remote-System anmelden, es sei denn, das Remote-System gestattet anonymes FTP.

  Sie können enorme Datenmengen von *anonymen FTP-Servern* beziehen, die mit dem Internet verbunden sind. Diese Server wurden unter anderem von Universitäten und anderen Institutionen eingerichtet, um der Öffentlichkeit Software, Forschungsunterlagen und andere Informationen zur Verfügung zu stellen. Wenn Sie sich bei diesen Servern anmelden, verwenden Sie den Anmeldenamen `anonymous`, daher die Bezeichnung „Anonymer FTP-Server."

  Die Verwendung von anonymem FTP und das Einrichten von anonymen FTP-Servern wird in diesem Handbuch nicht beschrieben. Anonymes FTP wird jedoch in vielen Büchern wie z. B. *The Whole Internet User's Guide & Catalog* ausführlich beschrieben. Anweisungen zum Verwenden von FTP finden Sie im *System Administration Guide: Network Services* . In der Manpage `ftp(1)` sind alle `ftp`-Befehlsoptionen beschrieben, die über den Befehlsinterpreter aufgerufen werden. In der Manpage `ftpd(1M)` sind alle Services beschrieben, die vom `in.ftpd`-Daemon bereitgestellt werden.

- **Telnet** – Mit dem Telnet-Protokoll können Terminals und terminalorientierte Prozesse über ein Netzwerk, das TCP/IP ausführt, miteinander kommunizieren. Dieses Protokoll ist als `telnet`-Programm auf lokalen Systemen und als `in.telnetd`-Daemon auf Remote-Computern umgesetzt. Telnet bietet eine Benutzeroberfläche, über die zwei Host zeichen- oder zeilenweise miteinander kommunizieren können. Telnet umfasst verschiedene Befehle, die in der Manpage `telnet(1)` ausführlich dokumentiert sind.

- **TFTP** – Das Trivial File Transfer Protocol (`tftp`) bietet ähnliche Funktionen wie `ftp`, aber das Protokoll stellt keine interaktive Verbindung wie `ftp` her. Aus diesem Grund können Benutzer nicht den Inhalt eines Verzeichnisses anzeigen oder Verzeichnisse wechseln. Ein Benutzer muss den vollständigen Namen einer zu kopierenden Datei kennen. Der Befehlssatz von `tftp` wird in der Manpage `tftp(1)` ausführlich beschrieben.

UNIX „r"-Befehle

Mit den UNIX „r"-Befehlen können Benutzer Befehle an ihren lokalen Computern eingeben, die auf dem Remote-Host ausgeführt werden. Dazu gehören die folgenden Befehle:

- `rcp`
- `rlogin`
- `rsh`

Hinweise zur Verwendung dieser Befehle finden Sie in den Manpages `rcp(1)`, `rlogin(1)` und `rsh(1)`.

Namen-Services

Oracle Solaris bietet die folgenden Namen-Services:

- **DNS** – Der Domain-Namen-Service (DNS) ist einer der Namen-Services, der vom Internet für TCP/IP-Netzwerke bereitgestellt wird. DNS führt die Auflösung von Hostnamen zu IP-Adressen durch. Darüber hinaus dient DNS als Datenbank für die Mail-Verwaltung. Eine vollständige Beschreibung dieses Services finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* . Weitere Informationen finden Sie in der Manpage `resolver(3RESOLV)`.
- `/etc`-**Dateien** – Dieses ursprünglich Host-basierte UNIX-Namen-System wurde für eigenständige UNIX-Computer entwickelt und dann für die Verwendung im Netzwerk übernommen. Viele alte UNIX-Betriebssysteme und Computer verwenden dieses System noch immer, obwohl es für große und komplexe Netzwerke ungeeignet ist.
- **NIS** – Der Network Information Service (NIS) wurde unabhängig von DNS entwickelt und hat eine etwas andere Aufgabe. Während der DNS Verbindungen vereinfacht, indem er Computernamen anstelle von numerischen IP-Adressen verwendet, konzentriert sich der NIS darauf, die Netzwerkverwaltung zu vereinfachen, indem er eine zentrale Steuerung verschiedener Netzwerkinformationen ermöglicht. NIS speichert Informationen zu Computernamen und Adressen, Benutzern, dem Netzwerk selbst und Netzwerkservices. Die NIS-Namespace-Informationen werden in NIS-Maps gespeichert. Weitere Informationen zur NIS-Architektur und zur NIS-Verwaltung finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

Verzeichnisservice

Oracle Solaris unterstützt das LDAP (Lightweight Directory Access Protocol) zusammen mit dem Sun Open Net Environment (Sun ONE) Directory Server sowie andere LDAP Directory Server. Der Unterschied zwischen einem Namen-Service und einem Verzeichnisservice liegt im Funktionsumfang. Ein Verzeichnisservice bietet den gleichen Funktionsumfang wie ein Namen-Service und verfügt darüber hinaus über erweiterte Funktionen. Lesen Sie dazu *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

Dateiservices

Das NFS-Anwendungsschichtprotokoll bietet Dateiservices für Oracle Solaris. Ausführliche Informationen zum NFS-Service finden Sie im *System Administration Guide: Network Services* .

Netzwerkverwaltung

Mit dem Simple Network Management Protocol (SNMP) können Sie das Layout Ihres Netzwerks und den Status der wichtigsten Computer anzeigen. Darüber hinaus können Sie mit SNMP komplexe Netzwerkstatistiken über Programme beziehen, die auf einer grafischen Benutzeroberfläche (GUI) basieren. Viele Unternehmen bieten Programmpakete zur Netzwerkverwaltung, die das SNMP umsetzen.

Routing-Protokolle

Das Routing Information Protocol (RIP) und das Router Discovery Server Protocol (RDISC) sind zwei verfügbare Routing-Protokolle für TCP/IP-Netzwerke. Eine vollständige Liste der verfügbaren Routing-Protokolle für Oracle Solaris 10 finden Sie in Tabelle 5–1 und Tabelle 5–2.

So verarbeiten TCP/IP-Protokolle die Datenkommunikation

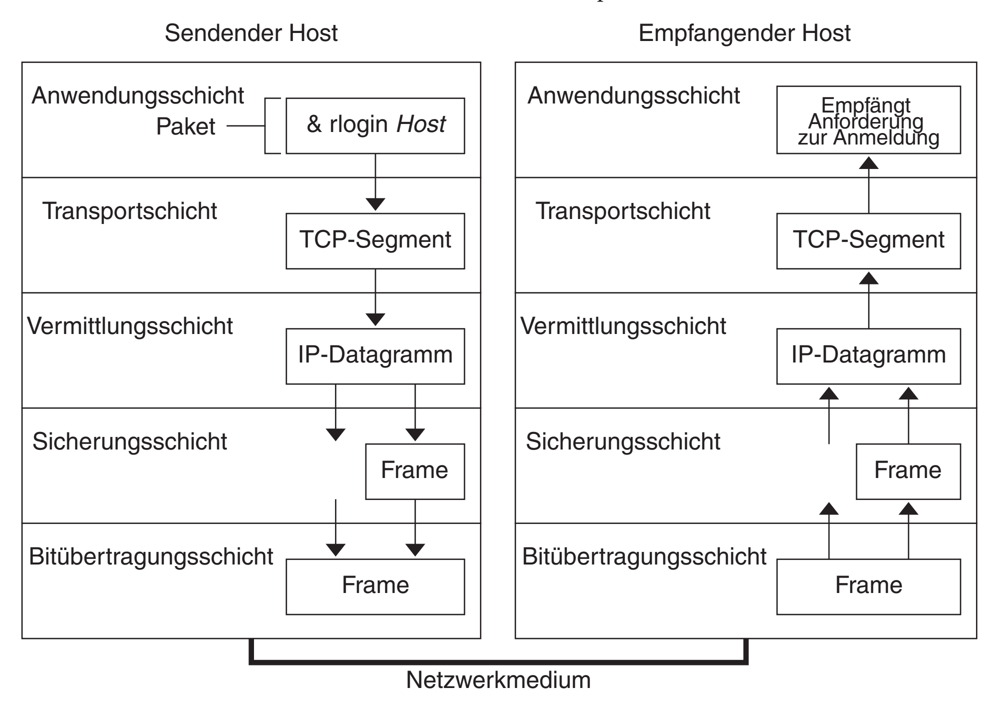
Gibt ein Benutzer einen Befehl ein, der ein Protokoll der TCP/IP-Anwendungsschicht verwendet, wird eine Abfolge von Ereignissen ausgelöst. Der Befehl oder die Nachricht des Benutzers durchläuft den TCP/IP-Protokollstapel auf dem lokalen System. Dann durchläuft der Befehl bzw. die Nachricht das Netzwerkmedium zu den Protokollen auf dem Remote-System. Auf jeder Schicht des sendenden Hosts fügen die Protokolle den ursprünglichen Daten Informationen hinzu.

Dann interagieren die Protokolle auf jeder Schicht des sendenden Hosts mit deren Peers auf dem empfangenden Host. Abbildung 1–1 zeigt diese Interaktion.

Datenkapselung und der TCP/IP-Protokollstapel

Das Paket ist die grundlegende Informationseinheit, die über ein Netzwerk übertragen wird. Ein allgemeines Paket besteht aus einem Header mit den Adressen des sendenden und empfangenden Systems sowie einem Body oder *Nutzlast* mit den zu übertragenden Daten. Während das Paket den TCP/IP-Protokollstapel durchläuft, werden durch die Protokolle auf den einzelnen Schichten entweder Felder zum Basis-Header hinzugefügt oder entfernt. Wenn ein Protokoll auf dem sendenden System Daten zum Paket-Header hinzufügt, wird dies als *Datenkapselung* bezeichnet. Jede Schicht vergibt einen anderen Begriff für das geänderte Paket. Dies wird in der folgenden Abbildung gezeigt.

ABBILDUNG 1–1 So durchläuft ein Paket durch den TCP/IP-Stapel



In diesem Abschnitt wird der Lebenszyklus eines Pakets beschrieben. Der Lebenszyklus beginnt, wenn Sie einen Befehl eingeben oder eine Nachricht senden. Der Lebenszyklus endet, wenn die entsprechende Anwendung auf dem empfangenden System das Paket empfängt.

Anwendungsschicht: Beginn der Datenkommunikation

Der Lebenszyklus eines Datenpakets beginnt, wenn ein Benutzer auf einem System eine Nachricht sendet oder einen Befehl eingibt, der auf ein Remote-System zugreifen muss. Das Anwendungsprotokoll formatiert das Paket so, dass das entsprechende Transportschichtprotokoll (TCP oder UDP) das Paket verarbeiten kann.

Angenommen, der Benutzer gibt einen `rlogin`-Befehl ein, um sich bei einem Remote-System anzumelden. Dies wird in Abbildung 1–1 gezeigt. Der `rlogin`-Befehl verwendet das TCP-Transportschichtprotokoll. TCP erwartet, Daten in Form eines Bytestroms zu empfangen, der die Informationen des Befehls enthält. Aus diesem Grund sendet `rlogin` diese Daten als einen TCP-Datenstrom.

Transportschicht: Beginn der Datenkapselung

Wenn die Daten an der Transportschicht eintreffen, beginnen die Protokolle auf dieser Schicht die Datenkapselung. Die Transportschicht kapselt die Anwendungsdaten in Transportprotokoll-Dateneinheiten.

Dann erzeugt das Transportschichtprotokoll einen virtuellen Datenfluss zwischen der sendenden und der empfangenden Anwendung, die durch die Transport-Portnummer unterschieden werden. Die Portnummer gibt einen *Port* an, einen dedizierten Speicherort für den Empfang oder das Senden von Daten. Darüber hinaus bietet die Transportprotokollschicht weitere Services, z. B. zuverlässige Datenzustellung in vorgegebener Reihenfolge. Das Endergebnis hängt davon ab, ob die Informationen von TCP, SCTP oder UDP verarbeitet werden.

TCP-Segmentierung

TCP wird häufig als „verbindungsorientiertes" Protokoll bezeichnet, da es die erfolgreiche Datenzustellung beim empfangenden Host sicherstellt. Abbildung 1–1 zeigt, wie das TCP-Protokoll den Datenstrom vom `rlogin`-Befehl empfängt. Dann teilt TCP die von der Anwendungsschicht empfangenen Daten in Segmente auf und fügt jedem Segment einen Header hinzu.

Die Segment-Header enthalten die Sende- und Empfangs-Ports, Informationen zur Reihenfolge der Segmente sowie ein Datenfeld, das als *checksum* (Prüfsumme) bezeichnet wird. Die TCP-Protokolle auf beiden Host stellen anhand der Prüfsumme fest, ob die Datenübertragung ohne Fehler erfolgt ist.

Herstellen einer TCP-Verbindung

TCP prüft anhand von Segmenten, ob das empfangende System zum Empfang von Daten bereit ist. Wenn der sendende Host eine Verbindung herstellen will, sendet das TCP-Protokoll ein Segment mit der Bezeichnung *SYN* an das TCP-Protokoll auf dem empfangenden Host. Dieser sendet über das TCP-Protokoll ein Segment mit der Bezeichnung *ACK* zurück, um den erfolgreichen Empfang des Segments zu bestätigen. Das sendende TCP sendet ein weiteres ACK-Segment und beginnt dann mit dem Senden der Daten. Dieser Austausch von Steuerungsinformationen wird als *Dreifach-Handshake* bezeichnet.

UDP-Pakete

UDP ist ein „verbindungsloses" Protokoll. Im Gegensatz zu TCP prüft UDP die am empfangenden Host eintreffenden Daten nicht. Stattdessen formatiert UDP die von der Anwendungsschicht empfangene Nachricht in *UDP-Pakete*. UDP fügt einen Header an jedes Paket an. Der Header enthält die sendenden und empfangenden Ports, ein Feld mit der Paketlänge sowie eine Prüfsumme.

Der sendende UDP-Prozessor versucht, das Paket an den UDP-Peer-Prozess auf dem empfangenden Host zu senden. Die Anwendungsschicht stellt fest, ob der empfangende UDP-Prozess den Empfang des Pakets bestätigt. UDP benötigt keine Benachrichtigung über den Empfang, und verwendet keinen Dreifach-Handshake.

Internetschicht: Vorbereitung der Pakete für die Zustellung

Die Transportprotokolle TCP, UDP und SCTP übergeben ihre Segmente und Pakete an die Internetschicht, auf der das IP-Protokoll die Segmente und Pakete weiter verarbeitet. Das IP-Protokoll bereitet die Segmente und Pakete für die Zustellung vor, indem es sie zu Einheiten zusammenfasst, die als *IP-Datagramme* bezeichnet werden. Dann legt das IP-Protokoll die IP-Adressen für die Datagramme fest, so dass sie korrekt an den empfangenden Host zugestellt werden können.

IP-Datagramme

Das IP-Protokoll hängt neben den Informationen, die vom TCP- oder UDP-Protokoll hinzugefügt wurden, einen *IP-Header* an das Segment bzw. den Header des Pakets an. Die Informationen im IP-Header umfassen die IP-Adressen des sendenden und des empfangenden Hosts, die Datagrammlänge sowie die Reihenfolge im Datagramm. Diese Informationen sind erforderlich, wenn das Datagramm die zulässige Bytegröße für Netzwerkpakete überschreitet und fragmentiert werden muss.

Sicherungsschicht: Durchführen des Framing

Die Protokolle der Sicherungsschicht, z. B. PPP, formatieren das IP-Datagramm als einen *Frame*. Diese Protokolle hängen einen dritten Header und einen Footer an den „Frame“ des Datagramms an. Der Frame-Header enthält ein Feld *cyclic redundancy check* (CRC) für die zyklische Blockprüfung, mit der auf Fehler geprüft wird, die während der Übertragung des Frames über die Netzwerkmedien aufgetreten sind. Dann übergibt die Sicherungsschicht den Frame an die Bitübertragungsschicht.

Bitübertragungsschicht: Senden und Empfangen von Frames

Die Bitübertragungsschicht auf dem sendenden Host empfängt die Frames und wandelt die IP-Adressen in für die Netzwerkmedien geeignete Hardware-Adressen um. Dann sendet die Bitübertragungsschicht den Frame über das Netzwerkmedium.

So verarbeitet der empfangende Host das Paket

Wenn das Paket auf dem empfangenden Host eintrifft, durchläuft es den TCP/IP-Protokollstapel in umgekehrter Sende-Reihenfolge. Dies wird in Abbildung 1–1 gezeigt. Darüber hinaus streift jedes Protokoll auf dem empfangenden Host die Header-Informationen ab, die von dessen Peer auf dem sendenden Host hinzugefügt wurden. Dabei läuft der folgende Prozess ab:

1. Die Bitübertragungsschicht empfängt das Paket im Frame-Format. Sie berechnet das CRC des Pakets und sendet den Frame dann an die Sicherungsschicht.
2. Die Sicherungsschicht prüft, ob das CRC für den Frame korrekt ist und streift dann den Frame-Header und das CRC ab. Schließlich sendet das Protokoll der Sicherungsschicht den Frame an die Sitzungsschicht.

3. Die Sitzungsschicht liest die Informationen im Header, um die Übertragung zu identifizieren. Anschließend stellt die Sitzungsschicht fest, ob es sich bei dem Paket um ein Fragment handelt. Wenn die Übertragung fragmentiert wurde, setzt das IP-Protokoll die Fragmente zum ursprünglichen Datagramm zusammen. Dann streift das IP-Protokoll den IP-Header ab und übergibt das Datagramm an die Protokolle der Transportschicht.
4. Die Protokolle der Transportschicht (TCP, SCTP und UDP) lesen den Header ein, um festzustellen, welches Protokoll der Anwendungsschicht die Daten empfangen muss. Dann streift TCP, SCTP oder UDP den entsprechenden Header ab. TCP, SCTP oder UDP sendete die Nachricht oder den Datenstrom an die empfangende Anwendung.
5. Die Anwendungsschicht empfängt die Nachricht. Abschließend führt die Anwendungsschicht den Vorgang aus, den der sendende Host angefordert hat.

TCP/IP Internal Trace-Unterstützung

TCP/IP unterstützt das Internal Tracing, indem es die TCP-Kommunikation protokolliert, wenn ein RST-Paket eine Verbindung beendet. Beim Senden oder Empfangen eines RST-Pakets werden die Informationen aus zehn gerade übertragenen Paketen zusammen mit den Verbindungsinformationen protokolliert.

Weitere Informationen zu TCP/IP und dem Internet

Informationen zu TCP/IP und dem Internet sind zahlreich vorhanden. Wenn Sie weitere Informationen zu den in diesem Kapitel angesprochenen Themen benötigen, werden Sie wahrscheinlich in den im Folgenden aufgeführten Quellen fündig.

Computerbücher über TCP/IP

Viele Bücher über TCP/IP und das Internet finden Sie in Ihrer lokalen Bücherei oder im Buchhandel. Die folgenden beiden Bücher gelten als Standardwerke zum Thema TCP/IP:

- Craig Hunt. *TCP/IP Network Administration* – Dieses Buch enthält einige theoretische und viele praktische Informationen zur Verwaltung eines heterogenen TCP/IP-Netzwerks.
- W. Richard Stevens. *TCP/IP Illustrated, Volume I* – Dieses Buch enthält detaillierte Beschreibungen der TCP/IP-Protokolle. Dieses Buch eignet sich ideal für Netzwerkadministratoren und -programmierer, die einen technischen Hintergrund zu TCP/IP benötigen.

Websites zum Thema TCP/IP und Arbeiten in Netzwerken

Im Internet finden sich viele Websites und Usergroups, die sich den TCP/IP-Protokollen und deren Verwaltung widmen. Viele Hersteller, einschließlich Oracle Corporation, bieten webbasierte Ressourcen mit allgemeinen TCP/IP-Informationen. Im Folgenden sind einige hilfreiche Web-Ressourcen mit Informationen zu TCP/IP und allgemeiner Systemverwaltung aufgeführt. In dieser Tabelle werden relevante Websites und die von diesen Websites bereitgestellten Vernetzungsinformationen aufgeführt.

Website	Beschreibung
Website der Internet Engineering Task Force (IETF) (`http://www.ietf.org/home.html`)	Die IETF ist für die Architektur und Überwachung des Internet verantwortlich. Die Website der IETF enthält Informationen zu den verschiedenen Aktivitäten dieser Organisation. Darüber hinaus enthält sie Links zu den wichtigsten Veröffentlichung in der IETF.
BigAdmin Portal von Oracle Corporation (`http://www.sun.com/bigadmin/home/index.jsp`)	BigAdmin bietet Informationen zur Verwaltung von Sun-Computern. Diese Site enthält häufig gestellte Fragen (FAQs), Ressourcen, Diskussionen, Links zu Dokumentationen sowie weiteres Material zur Verwaltung von Oracle Solaris 10, einschließlich dem Arbeiten in Netzwerken.

Requests for Comments und Internet Drafts

Die Arbeitsgruppen der Internet Engineering Task Force (IETF) veröffentlichen Standarddokumente, die als *Requests for Comments* (RFCs) bezeichnet werden. Im Entwurf befindliche Standards werden in so genannten *Internet Drafts* veröffentlicht. Das Internet Architecture Board (IAB) muss alle RFCs genehmigen, bevor sie der Öffentlichkeit vorgestellt werden. Im Allgemeinen richten sich RFCs und Internet Drafts an Entwickler und andere technisch interessierte Leser. Verschiedene RFCs, die sich mit dem TCP/IP befassen, enthalten auch für Systemadministratoren wertvolle Informationen. Diese RFCs werden an verschiedenen Stellen in diesem Handbuch zitiert.

Im Allgemeinen erscheinen „For Your Information“ (FYI)-Dokumente (etwa = Nur zur Information) als eine Untergruppe der RFCs. FYIs enthalten Informationen, die sich nicht auf Internetstandards beziehen. FYIs enthalten allgemeinere Informationen zum Internet. Beispielsweise enthalten sie eine Bibliothek, in der Bücher und Unterlagen aufgeführt sind, die in das Thema TCP/IP einführen. FYI-Dokumente sind ein umfassendes Kompendium

Internet-bezogener Softwaretools. Darüber hinaus enthalten FYI-Dokumente ein Glossar mit Begriffen aus dem Internet und allgemeinen Netzwerk-Begriffen.

Verweise auf die jeweiligen RFCs finden Sie im gesamten Handbuch und in anderen Büchern der Oracle Solaris System Administrator-Collection.

TEIL II

Administration von TCP/IP

Dieser Teil enthält Aufgaben und konzeptuelle Informationen zur Konfiguration, Verwaltung und Fehlerbehebung in TCP/IP-Netzwerken.

Planen Ihres TCP/IP-Netzwerks (Vorgehen)

In diesem Kapitel werden die Fragen beschrieben, die beim Erstellen eines strukturierten und kosteneffektiven Netzwerks auftreten können. Nachdem Sie diese Fragen beantwortet haben, können Sie einen Netzwerkplan entwerfen, wie Ihr zukünftiges Netzwerk konfiguriert und verwaltet werden soll.

Dieses Kapitel enthält die folgenden Informationen:

- „Festlegen der Netzwerkhardware“ auf Seite 57
- „Beziehen der IP-Adresse Ihres Netzwerks“ auf Seite 60
- „Festlegen eines IP-Adressierungsformats für Ihr Netzwerk“ auf Seite 58
- „Benennen von Entitäten in Ihrem Netzwerk“ auf Seite 66
- „Planen der Router für Ihr Netzwerk“ auf Seite 69

Die Aufgaben bei der Konfiguration eines Netzwerks finden Sie in Kapitel 5, „Konfiguration der TCP/IP-Netzwerkservices und IPv4-Adressierung (Aufgaben)“.

Netzwerkplanung (Übersicht der Schritte)

In der folgenden Tabelle sind verschiedene Aufgaben beschrieben, die zum Konfigurieren des Netzwerks erforderlich sind. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen Aufgaben sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Weitere Informationen
1. Planen der Hardwareanforderungen und der Netzwerktopologie	Ermitteln Sie die erforderlichen Geräte und das Layout dieser Geräte an Ihrem Standort.	■ Antworten auf allgemeine Fragen zur Netzwerktopologie finden Sie unter „Festlegen der Netzwerkhardware“ auf Seite 57. ■ Informationen zur Planung einer IPv6-Topologie finden Sie unter „Vorbereiten der Netzwerktopologie auf die Unterstützung von IPv6“ auf Seite 93. ■ Allgemeine Informationen zu einem bestimmten Gerät entnehmen Sie bitte der Dokumentation des Gerätsherstellers.
2. Beziehen einer registrierten IP-Adresse für Ihr Netzwerk	Wenn Sie beabsichtigen, mit Geräten außerhalb Ihres lokalen Netzwerks zu kommunizieren (z. B. über das Internet), muss Ihr Netzwerk über eine einmalige IP-Adresse verfügen.	Lesen Sie dazu „Beziehen der IP-Adresse Ihres Netzwerks“ auf Seite 60.
3. Entwerfen eines IP-Adressierungsschemas für Ihre Systeme, basierend auf dem IPv4-Netzwerkpräfix oder dem IPv6-Standortpräfix.	Legen Sie fest, wie Adressen an Ihrem Standort bereitgestellt werden.	Lesen Sie dazu „Erstellen eines IPv4-Adressierungsschemas“ auf Seite 61 oder „Vorbereiten eines IPv6-Adressierungsplans“ auf Seite 98.
4. Erstellen einer Liste mit den IP-Adressen und Hostnamen aller Computer in Ihrem Netzwerk.	Erstellen Sie mit dieser Liste die Netzwerkdatenbanken.	Lesen Sie dazu „Netzwerkdatenbanken“ auf Seite 67.
5. Festlegen des Namen-Service in Ihrem Netzwerk.	Legen Sie fest, ob NIS, LDAP, DNS oder die Netzwerkdatenbanken im lokalen `/etc`-Verzeichnis verwendet werden sollen.	Lesen Sie dazu „Auswählen eines Namen- und Verzeichnisservices“ auf Seite 67.
6. Einrichten von administrativen Unterbereichen, sofern dies für Ihr Netzwerk zutrifft.	Entscheiden Sie, ob das Netzwerk an Ihrem Standort in administrative Unterbereiche aufgeteilt werden muss.	Lesen Sie dazu „Administrative Unterbereiche“ auf Seite 68.

Aufgabe	Beschreibung	Weitere Informationen
7. Festlegen, an welchen Stellen im Netzwerkentwurf Router platziert werden müssen.	Wenn Ihr Netzwerk so groß ist, dass Router erforderlich sind, erstellen Sie eine Netzwerktopologie, die Router unterstützt.	Lesen Sie dazu „Planen der Router für Ihr Netzwerk“ auf Seite 69.
8. Falls erforderlich, entwerfen Sie eine Strategie für Teilnetze.	Eventuell müssen Sie Teilnetze zur Verwaltung Ihres IP-Adressraums erstellen oder mehr IP-Adressen für Benutzer verfügbar machen.	Informationen zur Planung von IPv4-Teilnetzen finden Sie unter „Was versteht man unter Subnetting?“ auf Seite 260 Informationen zur Planung von IPv6-Teilnetzen finden Sie unter „Erstellen eine Nummerierungsschemas für Teilnetze“ auf Seite 98

Festlegen der Netzwerkhardware

Bei der Planung Ihres Netzwerks müssen Sie entscheiden, welcher Netzwerktyp die Anforderungen Ihres Unternehmens am besten erfüllt. Einige der von Ihnen zu treffenden Entscheidungen betreffen die folgende Netzwerkhardware:

- Die Netzwerktopologie, das Layout und die Verbindungen der Netzwerkhardware
- Die Anzahl der Hostsysteme, die Ihr Netzwerk unterstützen kann
- Die vom Netzwerk unterstützten Hosttypen
- Die benötigten Servertypen
- Den Typ der zu verwendenden Netzwerkmedien: Ethernet, Token Ring, FDDI usw.
- Ob Brücken oder Router erforderlich sind, um das Netzwerk zu erweitern oder um das lokale Netzwerk mit externen Netzwerken zu verbinden
- Ob für bestimmte Systeme neben den integrierten Schnittstellen separat erworbene Schnittstellen erforderlich sind

Auf Grundlage dieser Faktoren können Sie die Größe Ihres lokalen Netzwerks feststellen.

Hinweis – Informationen zur Planung der Netzwerkhardware sind in diesem Handbuch nicht enthalten. Lesen Sie dazu die Handbücher der von Ihnen erworbenen Netzwerkhardware.

Festlegen eines IP-Adressierungsformats für Ihr Netzwerk

Die Konfiguration Ihres Netzwerks hängt unter anderem von der Anzahl der zu unterstützenden Systeme ab. Vielleicht ist für Ihr Unternehmen nur ein kleines Netzwerk mit mehreren Dutzend eigenständiger Systeme erforderlich, die sich alle in einem Stockwerk eines einzelnen Gebäudes befinden. Sie müssen eventuell auch ein Netzwerk mit mehr als 1000 Systemen in mehreren Gebäuden einrichten. In diesem Fall müssen Sie Ihr Netzwerk wahrscheinlich in so genannte *Teilnetze* (Subnets) unterteilen.

Bei der Planung des Netzwerk-Adressierungsschemas müssen folgende Faktoren berücksichtigt werden:

- Die Art der IP-Adresse, die Sie verwenden wollen: IPv4 oder IPv6
- Die Anzahl der potentiellen Systemen in Ihrem Netzwerk
- Die Anzahl der Systeme mit mehreren IP-Adressen oder Router, die für jede Schnittstelle eine IP-Adresse benötigen
- Ob private Adressen in Ihrem Netzwerk verwendet werden
- Ob ein DHCP-Server vorhanden ist, der IPv4-Adresspools verwaltet

Das weltweite Wachstum des Internets seit 1990 hat dazu geführt, dass die verfügbaren IP-Adressen mittlerweile knapp werden. Als Abhilfe hat die Internet Engineering Task Force (IETF) eine Reihe von IP-Adressierungsalternativen entwickelt. Die heute üblichen IP-Adresstypen sind:

Wenn Ihr Unternehmen mehrere IP-Adressen für das Netzwerk zugewiesen hat oder Teilnetze verwendet, wählen Sie eine zentrale Stelle im Unternehmen aus, die die Netzwerk-IP-Adressen zuordnet. Diese Stelle muss einen Pool mit zugewiesenen Netzwerk-IP-Adressen verwalten und auf Anforderung Netzwerk-, Teilnetz- und Host-Adressen zuordnen können. Um Probleme zu vermeiden, müssen Sie sicherstellen, dass in Ihrem Unternehmen keine doppelten oder zufällig erzeugten Netzwerknummern existieren.

IPv4-Adressen

Diese 32-Bit-Adressen sind das ursprüngliche, für TCP/IP entworfene IP-Adressierungsformat. Ursprünglich weisen IP-Netzwerke drei Klassen auf: A, B und C. Die einem Netzwerk zugewiesene *Netzwerknummer* spiegelt die Klassenzuweisung wieder, plus 8 oder mehr Bit, um einen Host zu repräsentieren. Klassenbasierte IPv4-Adressen erfordern die Konfiguration einer Netzmaske für die Netzwerknummer. Darüber hinaus werden diese Adressen häufig in Teilnetze aufgeteilt, damit mehr Adressen für Systeme im lokalen Netzwerk zur Verfügung stehen.

Heutzutage werden IP-Adressen als *IPv4-Adressen* bezeichnet. Obwohl Sie keine klassenbasierten IPv4-Netzwerknummern mehr von einem ISP beziehen können, sind sie noch

immer in existierenden Netzwerken vorhanden. Weitere Informationen zur Verwaltung von IPv4-Adressen finden Sie unter „Erstellen eines IPv4-Adressierungsschemas“ auf Seite 62.

IPv4-Adressen im CIDR-Format

Die IETF hat Classless Inter-Domain Routing (CIDR)-Adressen als kurz- bzw. mittelfristige Lösung für den Mangel an IPv4-Adressen entwickelt. Außerdem wurde das CIDR-Format entworfen, um den Mangel an Kapazität der globalen Internet-Routing-Tabellen zu beseitigen. Eine IPv4-Adresse in der CIDR-Notation ist 32 Bit lang und verfügt über die gleiche dezimale getrennte Notation. CIDR fügt jedoch eine Präfix-Zuweisung hinter dem rechten Byte hinzu, um den Netzwerkteil der IPv4-Adresse zu definieren. Weitere Informationen hierzu finden Sie unter „Erstellen eines CIDR IPv4-Adressierungsschemas“ auf Seite 64.

DHCP-Adressen

Das Dynamic Host Configuration Protocol (DHCP)-Protokoll ermöglicht es einem System, Konfigurationsinformationen (einschließlich einer IP-Adresse) als Teil des Boot-Prozesses von einem DHCP-Server zu beziehen. DHCP-Server verwalten IP-Adresspools, aus denen den DHCP-Clients Adressen zugewiesen werden. Ein Standort, an dem DHCP verwendet wird, kann einen Pool mit IP-Adressen verwenden, der kleiner ist als eine Konfiguration, bei der allen Clients eine permanente IP-Adresse zugewiesen wird. Sie können den Oracle Solaris DHCP-Service so einrichten, dass er entweder alle IP-Adressen an Ihrem Standort oder nur einen Teil dieser Adressen verwaltet. Weitere Informationen hierzu finden Sie in Kapitel 12, „Einführung in Oracle Solaris DHCP“.

IPv6-Adressen

Die IETF hat IPv6-Adressen mit einer Länge von 128 Bit als langfristige Lösung für den Mangel an verfügbaren IPv4-Adressen entwickelt. IPv6-Adressen bieten einen größeren Adressraum als IPv4. Oracle Solaris unterstützt IPv4- und IPv6-Adressierung auf dem gleichen Host mithilfe eines TCP/IP-Dual Stack. Wie IPv4-Adressen im CIDR-Format sind sich auch IPv6-Adressen Netzwerkklassen oder Netzmasken nicht bewusst. Wie bei CIDR verwenden IPv6-Adressen Präfixe, um den Teil der Adresse zu kennzeichnen, der das Netzwerk am Standort definiert. Eine Einführung in IPv6 finden Sie unter „Einführung in die IPv6-Adressierung“ auf Seite 78.

Private Adressen und Dokumentationspräfixe

Die IANA hat einen Block von IPv4-Adressen und ein IPv6-Standortpräfix für die Verwendung in privaten Netzwerken reserviert. Sie können diese Adressen auf Systemen in einem

Unternehmensnetzwerk bereitstellen, müssen aber berücksichtigen, dass Pakete mit privaten Adressen nicht über das Internet geleitet werden können. Weitere Informationen zu privaten Adressen finden Sie unter „Verwenden privater IPv4-Adressen“ auf Seite 65.

Hinweis – Private IPv4-Adressen werden auch für Dokumentationszwecke verwendet. Die Beispiele in diesem Buch verwenden private IPv4-Adressen und das reservierte IPv6-Dokumentationspräfix.

Beziehen der IP-Adresse Ihres Netzwerks

Ein IPv4-Netzwerk wird durch die Kombination einer IPv4-Netzwerknummer plus einer Netzwerkmaske oder *Netzmaske* definiert. Ein IPv6-Netzwerk wird von seinem *Standortpräfix* und (falls es ein Teilnetz ist) *Teilnetzpräfix* definiert.

Wenn Ihr Netzwerk nicht für alle Zeiten privat bleiben soll, müssen die lokalen Benutzer in der Lage sein, über das lokale Netzwerk hinaus zu kommunizieren. Damit Ihr Netzwerk extern kommunizieren kann, müssen Sie eine registrierte IP-Adresse für Ihr Netzwerk von einer entsprechenden Organisation beziehen. Diese Adresse wird die Netzwerknummer für Ihr IPv4-Adressierungsschema oder das Standortpräfix für Ihr IPv6-Adressierungsschema.

Internet Service Provider bieten IP-Adressen für Netzwerke zu Preisen an, die auf den in Anspruch genommenen Services beruhen. Nehmen Sie mit verschiedenen ISPs Kontakt auf, um festzustellen, welcher Anbieter den besten Service für Ihr Netzwerk anbietet. ISPs bieten Geschäftskunden in der Regel dynamisch zugewiesene Adressen oder statische IP-Adressen. Einige ISPs bieten sowohl IPv4- als auch IPv6-Adressen an.

Falls Ihr Unternehmen ein ISP ist, können Sie IP-Adressblöcke für Ihre Kunden von Ihrer lokalen Internet Registry (IR) beziehen. Die Internet Assigned Numbers Authority (IANA) ist letztlich für die Delegierung von registrierten IP-Adressen an IRs verantwortlich. Jede IR verfügt über Registrierungsinformationen und -vorlagen für das Gebiet, das sie versorgt. Informationen zu IANA und deren IRs finden Sie auf der IANA-Service-Seite zu IP-Addressen (`http://www.iana.org/ipaddress/ip-addresses.htm`).

Hinweis – Weisen Sie in Ihrem Netzwerk nicht willkürlich IP-Adressen zu, auch dann nicht, wenn Sie das Netzwerk momentan nicht mit externen TCP/IP-Netzwerken verbinden. Verwenden Sie in diesem Fall die unter „Verwenden privater IPv4-Adressen“ auf Seite 65 beschriebenen privaten Adressen.

Erstellen eines IPv4-Adressierungsschemas

Hinweis – Informationen zur Planung von IPv6-Adressen finden Sie unter „Vorbereiten eines IPv6-Adressierungsplans“ auf Seite 98.

Dieser Abschnitt enthält eine allgemeine Einführung in die IPv4-Adressierung, um Sie bei der Erstellung eines IPv4-Adressierungsplans zu unterstützen. Weitere Informationen zu IPv6-Adressen finden Sie unter „Einführung in die IPv6-Adressierung“ auf Seite 78. Weitere Informationen zu DHCP-Adressen finden Sie in Kapitel 12, „Einführung in Oracle Solaris DHCP“.

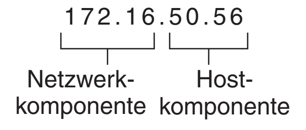
Jedes IPv4-basierte Netzwerk muss über Folgendes verfügen:

- Eine einmalige Netzwerknummer, die entweder von einem ISP oder einer IR zugewiesen wird, oder - bei älteren Netzwerken - von der IANA registriert wird. Wenn Sie private Adressen verwenden möchten, müssen die von Ihnen verwendeten Netzwerknummern innerhalb Ihres Unternehmens einmalig sein.
- Einmalige IPv4-Adressen für die Schnittstellen jedes Systems im Netzwerk.
- Eine Netzwerkmaske.

Eine IPv4-Adresse ist eine 32-Bit-Adresse, die eine Netzwerkschnittstelle in einem System eindeutig identifiziert. Dies wird unter „Anwenden von IP-Adressen für Netzwerkschnittstellen“ auf Seite 65 ausführlich beschrieben. Eine IPv4-Adresse wird in Dezimalzahlen geschrieben, aufgeteilt in vier 8-Bit-Felder, die durch Punkte voneinander getrennt sind. Jedes 8-Bit-Feld repräsentiert ein Byte der IPv4-Adresse. Dieses Format der Darstellung der Byte einer IPv4-Adresse wird auch als *getrennte dezimale Notation* bezeichnet.

Die folgende Abbildung zeigt die Komponenten der IPv4-Adresse `172.16.50.56`.

ABBILDUNG 2–1 IPv4-Adressformat



`172.16` Registrierte IPv4-Netzwerknummer. Bei einer klassenbasierten IPv4-Notation definiert diese Nummer auch die IP-Netzwerkklasse (in diesem Beispiel Klasse B), die von der IANA registriert worden wäre.

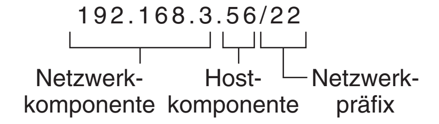
`50.56` Hostkomponente der IPv4-Adresse. Die Hostkomponente identifiziert eine Schnittstelle eines Systems in einem Netzwerk eindeutig. Beachten Sie, dass bei jeder Schnittstelle in einem lokalen Netzwerk die Netzwerkkomponente der

Adresse gleich ist, die Hostkomponente jedoch unterschiedlich sein muss.

Wenn Sie ein Teilnetz für ein klassenbasiertes IPv4-Netzwerk planen, müssen Sie eine Teilnetzmaske bzw. eine *Netzmaske* definieren. Dies wird unter „`netmasks`-Datenbank“ auf Seite 260 ausführlich beschrieben.

Das nächste Beispiel zeigt eine Adresse im CIDR-Format: `192.168.3.56/22`

ABBILDUNG 2–2 IPv4-Adresse im CIDR-Format



`192.168.3`	Netzwerkteil, der aus der IPv4-Netzwerknummer besteht, die von einem ISP oder einer IR bezogen wurde.
`56`	Hostteil, den Sie einer Schnittstelle im System zuweisen.
`/22`	Netzwerkpräfix, das definiert, wie viele Bit der Adresse die Netzwerknummer ausmachen. Das Netzwerkpräfix stellt außerdem die Teilnetzmaske für die IP-Adresse zur Verfügung. Netzwerkpräfixe werden ebenfalls vom ISP oder einer IR zugewiesen.

In einem Oracle Solaris-basierten Netzwerk können standardmäßige IPv4-Adressen, IPv4-Adressen im CIDR-Format, DHCP-Adressen, IPv6-Adressen und private IPv4-Adressen kombiniert werden.

Erstellen eines IPv4-Adressierungsschemas

In diesem Abschnitt werden die Klassen beschrieben, in denen standardmäßige IPv4-Adressen organisiert sind. Obwohl die IANA keine klassenbasierten Netzwerknummern mehr ausgibt, werden diese Netzwerknummern noch immer in vielen Netzwerken verwendet. Eventuell müssen Sie den Adressraum für einen Standort mit klassenbasierten Netzwerknummern verwalten. Eine vollständige Diskussion von IPv4-Netzwerkklassen finden Sie unter „Netzwerkklassen“ auf Seite 274.

In der folgenden Tabelle wird die Aufteilung einer standardmäßigen IPv4-Adresse in die Netzwerk- und Host-Adressräume gezeigt. Bei jeder Klasse gibt „Bereich“ den Bereich der Dezimalzahlen für das erste Byte der Netzwerknummer an. „Netzwerkadresse“ gibt die Anzahl der Byte der IPv4-Adresse an, die dem Netzwerkteil der Adresse zugewiesen sind. Jedes Byte wird durch *xxx* dargestellt. „Hostadresse“ gibt die Anzahl der Byte der IPv4-Adresse an, die dem Hostteil der Adresse zugewiesen sind. Beispielsweise ist bei einer Netzwerkadresse der

Klasse A das erste Byte für das Netzwerk vorgesehen und die letzten drei Byte für den Host. Für ein Netzwerk der Klasse C gilt eine umgekehrte Zuweisung.

TABELLE 2–1 Aufteilung der IPv4-Klassen

Klasse	Byte-Bereich	Netzwerknummer	Hostadresse
A	0–127	*xxx*	*xxx.xxx. xxx*
B	128–191	*xxx.xxx*	*xxx.xxx*
C	192–223	*xxx.xxx. xxx*	*xxx*

Die Zahlen im ersten Byte der IPv4-Adresse definieren, ob es sich bei dem Netzwerk um ein Netzwerk der Klasse A, B oder C handelt. Die übrigen drei Byte haben einen Bereich von 0–255. Die zwei Zahlen 0 und 255 sind reserviert. Sie können jedem Byte die Zahlen 1–254 zuweisen, abhängig von der Netzwerkklasse, die Ihrem Netzwerk von der IANA zugewiesen wurde.

In der folgenden Tabelle wird gezeigt, welche Byte der IPv4-Adresse für Sie zugewiesen sind. Außerdem zeigt die Tabelle den Zahlenbereich innerhalb jedes Byte, der Ihnen zum Zuweisen zu Ihren Hosts zur Verfügung steht.

TABELLE 2–2 Bereich der verfügbaren IPv4-Klassen

Netzwerkklasse	Byte 1-Bereich	Byte 2-Bereich	Byte 3-Bereich	Byte 4-Bereich
A	0–127	1–254	1–254	1–254
B	128–191	Vorab zugewiesen durch IANA	1–254	1–254
C	192–223	Vorab zugewiesen durch IANA	Vorab zugewiesen durch IANA	1–254

IPv4-Teilnetznummer

Lokale Netzwerke mit zahlreichen Hosts sind häufig in Teilnetze unterteilt. Wenn Sie Ihre IPv4-Netzwerknummer in Teilnetze aufteilen, müssen Sie jedem Teilnetz einen Netzwerkbezeichner zuweisen. Sie können die Effizienz des IPv4-Adressraums maximieren, indem Sie einige Bit der Hostkomponente der IPv4-Adresse als Netzwerkbezeichner verwenden. Wenn Sie einen Netzwerkbezeichner verwenden, wird die angegebene Komponente der Adresse zur Teilnetznummer. Sie können eine Teilnetznummer mithilfe einer Netzmaske erstellen, eine Bitmaske, die die Netzwerk- und Teilnetzteile einer IPv4-Adresse auswählt. Weitere Informationen finden Sie unter „Erstellen der Netzwerkmaske für IPv4-Adressen“ auf Seite 261.

Erstellen eines CIDR IPv4-Adressierungsschemas

Die Netzwerkklassen, die ursprünglich IPv4 darstellten, werden im globalen Internet nicht mehr verwendet. Heute verteilt die IANA klassenlose Adressen im CIDR-Format an die weltweiten Registrierungsstellen. Alle IPv4-Adressen, die Sie von einem ISP beziehen, liegen in dem CIDR-Format vor, das in Abbildung 2–2 gezeigt wurde.

Das Netzwerkpräfix der CIDR-Adresse gibt an, wie viele IPv4-Adressen für Hosts in Ihrem Netzwerk zur Verfügung stehen. Diese Host-Adressen werden den Schnittstellen auf einem Host zugewiesen. Verfügt ein Host über mehrere physikalische Schnittstellen, müssen Sie jeder verwendeten physikalischen Schnittstelle eine eigene Host-Adresse zuweisen.

Das Netzwerkpräfix einer CIDR-Adresse definiert auch die Länge der Teilnetzmaske. Die meisten Oracle Solaris 10-Befehle erkennen die CIDR-Präfixzuweisung der Teilnetzmaske eines Netzwerks. Das Oracle Solaris-Installationsprogramm und die Datei `/etc/netmask` erfordern jedoch, dass Sie die Teilnetzmaske mithilfe der getrennten dezimalen Notation einrichten. In diesen beiden Fällen verwenden Sie die getrennte dezimale Notation des CIDR-Netzwerkpräfix, wie in der folgenden Tabelle gezeigt.

TABELLE 2–3 CIDR-Präfixe und deren Dezimalentsprechungen

CIDR-Netzwerkpräfix	Verfügbare IP-Adressen	Teilnetz-Entsprechung bei getrennter dezimaler Notation
/19	8192	255.255.224.0
/20	4096	255.255.240.0
/21	2048	255.255.248.0
/22	1024	255.255.252.0
/23	512	255.255.254.0
/24	256	255.255.255.0
/25	128	255.255.255.128
/26	64	255.255.255.192
/27	32	255.255.255.224

Weitere Informationen zu CIDR-Adressen finden Sie in den folgenden Quellen:

- Ausführliche technische Informationen zu CIDR finden Sie unter RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy (`http://www.ietf.org/rfc/rfc1519.txt?number=1519`).
- Allgemeine Information zu CIDR finden Sie bei Pacific Bell Internet unter Classless Inter-Domain Routing (CIDR) Overview (`http://www.wirelesstek.com/cidr.htm`).

- Eine weitere Übersicht zu·CIDR finden Sie im Wikipedia-Artikel unter "Classless Inter-Domain Routing" (`http://de.wikipedia.org/wiki/Classless_Inter-Domain_Routing`).

Verwenden privater IPv4-Adressen

Die IANA hat drei Blöcke mit IPv4-Adressen reserviert, die in privaten Netzwerken verwendet werden können. Diese Adressen sind in RFC 1918, Address Allocation for Private Internets (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`) definiert. Sie können diese *privaten Adressen*, die auch als 1918-Adressen bezeichnet werden, für Systeme in lokalen Netzwerken innerhalb eines Firmen-Intranets verwenden. Diese privaten Adressen sind jedoch im Internet nicht gültig. Verwenden Sie diese Adressen nicht auf Systemen, die mit Systemen außerhalb des lokalen Netzwerks kommunizieren müssen.

In der folgenden Tabelle werden die privaten IPv4-Adressbereiche und die entsprechenden Netzmasken aufgeführt.

IPv4-Adressbereich	Netzmaske
10.0.0.0 - 10.255.255.255	10.0.0.0
172.16.0.0 - 172.31.255.255	172.16.0.0
192.168.0.0 - 192.168.255.255	192.168.0.0

Anwenden von IP-Adressen für Netzwerkschnittstellen

Zum Herstellen einer Verbindung mit einem Netzwerk muss ein System über mindestens eine *physikalische Netzwerkschnittstelle* verfügen. Jede Netzwerkschnittstelle muss eine eigene, einmalige IP-Adresse aufweisen. Bei der Oracle Solaris-Installation geben Sie die IP-Adresse der ersten Schnittstelle an, die das Installationsprogramm findet. Im Allgemeinen hat diese Schnittstelle den Namen *Gerätename*0, z. B. `eri0` oder `hme0`. Diese Schnittstelle wird als *primäre Netzwerkschnittstelle* betrachtet.

Wenn Sie einem Host eine zweite Netzwerkschnittstelle hinzufügen, muss auch diese Schnittstelle eine eigene, einmalige IP-Adresse aufweisen. Dadurch wird der Host zu einem *Multihomed*-Host. Andererseits, wenn Sie einem Host eine zweite Netzwerkschnittstelle hinzufügen und die IP-Weiterleitung aktivieren, wird der Host zu einem Router. Eine Beschreibung finden Sie unter „Konfiguration eines IPv4-Routers“ auf Seite 126.

Jede Netzwerkschnittstelle besitzt einen Gerätenamen, einen Gerätetreiber sowie eine zugewiesene Gerätedatei im Verzeichnis `/devices.` Die Netzwerkschnittstelle weist einen Gerätenamen wie `eri` oder `smc0` auf; hierbei handelt es sich um Gerätenamen für zwei häufig verwendete Ethernet-Schnittstellen.

Weitere Informationen und Aufgaben im Zusammenhang mit Schnittstellen finden Sie unter „Verwalten der Schnittstellen in Solaris 10 3/05“ auf Seite 147 oder in Kapitel 6, „Verwalten von Netzwerkschnittstellen (Aufgaben)“.

Hinweis – In diesem Buch wird davon ausgegangen, dass Ihre Systeme über Ethernet-Netzwerkschnittstellen verfügen. Wenn Sie mit anderen Netzwerkmedien arbeiten möchten, entnehmen Sie die Informationen zur Konfiguration dieser Medien den Unterlagen, die mit den Netzwerkschnittstellen ausgeliefert wurden.

Benennen von Entitäten in Ihrem Netzwerk

Nachdem Sie die Ihnen zugewiesene IP-Netzwerkadresse empfangen und die IP-Adressen an Ihre Systeme verteilt haben, besteht die nächste Aufgabe darin, den Hosts Namen zuzuweisen. Dann müssen Sie festlegen, wie Namen-Services in Ihrem Netzwerk abgewickelt werden. Sie können diese Namen verwenden, wenn Sie Ihr Netzwerk einrichten und später, wenn Sie Ihr Netzwerk über Router, Brücken oder PPP erweitern.

Die TCP/IP-Protokolle lokalisieren ein System über die zugehörige IP-Adresse im Netzwerk. Sie können jedoch einen wiedererkennbaren Namen verwenden, an dem Sie das System einfach erkennen können. Aus diesem Grund erfordern die TCP/IP-Protokolle (und Oracle Solaris) sowohl die IP-Adresse als auch den Hostnamen, um ein System eindeutig zu identifizieren.

Aus der TCP/IP-Perspektive ist ein Netzwerk eine Reihe von benannten Entitäten. Ein Host ist eine Entität mit einem Namen. Ein Router ist eine Entität mit einem Namen. Ein Netzwerk ist eine Entität mit einem Namen. Eine Gruppe oder eine Abteilung, in dem das Netzwerk installiert wird, kann ebenfalls einen Namen erhalten wie auch eine Division, Region oder ein Unternehmen. Theoretisch kann eine Namenshierarchie verwendet werden, um ein praktisch unbegrenztes Netzwerk zu identifizieren. Der Domänename identifiziert eine *Domäne*.

Verwalten von Hostnamen

Viele Standorte lassen die Benutzer die Hostnamen für ihre Computer auswählen. Auch Server erfordern mindestens einen Hostnamen, der der IP-Adresse ihrer primären Netzwerkschnittstelle zugeordnet ist.

Als Systemadministrator müssen Sie sicherstellen, dass jeder Hostnamen in Ihrer Domäne einmalig ist. Mit anderen Worten, es dürfen keine zwei Computer in Ihrem Netzwerk den Namen „Fred” aufweisen. Andererseits kann der Computer „Fred“ über mehrere IP-Adressen verfügen.

Legen Sie bei der Planung Ihres Netzwerks eine Liste der IP-Adressen und der dazugehörigen Hostnamen an, damit Sie während des Setups problemlos auf die Computer zugreifen können. Die Liste hilft Ihnen auch, sicherzustellen, dass alle Hostnamen einmalig sind.

Auswählen eines Namen- und Verzeichnisservices

Oracle Solaris ermöglicht Ihnen die Auswahl unter drei Arten von Namen-Services: lokale Dateien, NIS und DNS. Namen-Services verwalten kritische Informationen zu Computern in einem Netzwerk, z. B. Hostnamen, IP-Adressen, Ethernet-Adressen usw. Mit Oracle Solaris können Sie den LDAP-Verzeichnisdienst zusätzlich oder anstelle eines Namen-Services verwenden. Eine Einführung in die Namen-Services in Oracle Solaris finden Sie in Teil I, „About Naming and Directory Services" in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Netzwerkdatenbanken

Bei der Installation des Betriebssystems geben Sie den Hostnamen und die IP-Adresse Ihres Servers, der Clients oder des eigenständigen Systems an. Das Oracle Solaris-Installationsprogramm fügt diese Informationen in die `Hosts`-Netzwerkdatenbank und bei Solaris 10 11/06 und früheren Solaris 10-Versionen in die `ipnodes`-Netzwerkdatenbank ein. Diese Datenbank ist Teil einer Reihe von Netzwerkdatenbanken, die für den TCP/IP-Betrieb in Ihrem Netzwerk erforderliche Informationen enthalten. Der von Ihnen für Ihr Netzwerk ausgewählte Namen-Service liest diese Datenbanken ein.

Die Konfiguration der Netzwerkdatenbanken ist entscheidend. Aus diesem Grund müssen Sie bereits während der Netzwerkplanung entscheiden, welcher Namen-Service verwendet werden soll. Außerdem wirkt sich die Entscheidung für einen Namen-Service darauf aus, ob Sie Ihr Netzwerk in administrativen Domänen strukturieren. Weitere Informationen zu den Netzwerkdatenbanken finden Sie unter „Netzwerkdatenbanken und die `nsswitch.conf`-Datei" auf Seite 264.

Verwenden von NIS oder DNS als Namen-Service

Die Namen-Services NIS und DNS verwalten Netzwerkdatenbanken auf mehreren Servern im Netzwerk. *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* beschreibt diese Namen-Services und erklärt die Konfiguration dieser Datenbanken. Darüber hinaus werden die Konzepte „Namespace" und „Administrationsdomäne" in diesem Handbuch ausführlich beschrieben.

Verwenden von lokalen Dateien als Namen-Service

Wenn Sie weder NIS, LDAP noch DNS implementieren, verwendet das Netzwerk *lokale Dateien* zur Bereitstellung des Namen-Services. Der Begriff „lokale Dateien" bezieht sich auf die

Dateien im Verzeichnis `/etc`, das von den Netzwerkdatenbanken verwendet wird. Sofern nicht anderweitig angegeben, wird bei den Verfahren in diesem Buch davon ausgegangen, dass Sie lokale Dateien als Namen-Service verwenden.

Hinweis – Wenn Sie sich entscheiden, lokale Dateien als Namen-Services für Ihr Netzwerk zu verwenden, können Sie zu einem späteren Zeitpunkt einen anderen Namen-Service einrichten.

Domänennamen

Viele Netzwerke strukturieren Hosts und Router in einer Hierarchie von Administrationsdomänen. Wenn Sie NIS oder DNS als Namen-Service verwenden, müssen Sie einen Domänennamen für Ihr Unternehmen wählen, der weltweit einmalig ist. Um sicherzustellen, dass Ihr Domänenname einmalig ist, müssen Sie den Domänennamen bei der InterNIC registrieren. Auch wenn Sie DNS verwenden möchten, müssen Sie Ihren Domänennamen bei der InterNIC registrieren.

Die Struktur des Domänennamens ist hierarchisch. Eine neue Domäne befindet sich in der Regel unter einer bereits vorhandenen, verwandten Domäne. So kann sich der Domänenname für ein Tochterunternehmen unter der Domäne der Muttergesellschaft befinden. Wenn der Domänenname keinerlei Beziehung aufweist, kann ein Unternehmen den Domänennamen direkt unter einer der vorhandenen Hauptdomänen (Top-Level-Domain) platzieren.

Im Folgenden sind einige Beispiele für Top-Level-Domains aufgeführt:

- `.com` – Kommerzielle Unternehmen (international)
- `.edu` – Bildungseinrichtungen (international)
- `.gov` – Behörden der US-Regierung
- `.de` – Deutschland

Sie können einen Namen wählen, der Ihr Unternehmen beschreibt, mit der Einschränkung, dass der Name einmalig sein muss.

Administrative Unterbereiche

Die Frage nach administrativen Unterteilungen befasst sich mit der Größe und Kontrollierbarkeit. Je mehr Hosts und Server in einem Netzwerk vorhanden sind, desto komplexer wird die Verwaltung. In diesen Fällen können Sie die Netzwerke durch Einrichten von zusätzlichen administrativen Unterteilungen besser verwalten. Fügen Sie Netzwerke einer bestimmten Klasse hinzu. Teilen Sie vorhandenen Netzwerke in Teilnetze auf. Ob Sie administrative Unterteilungen für Ihr Netzwerk einrichten, hängt von den folgenden Faktoren ab:

- **Wie groß ist das Netzwerk?**

Eine einzelne administrative Unterteilung kann ein einzelnes Netzwerk mit mehreren hundert Hosts umfassen, die sich alle am gleichen Standort befinden und die gleichen administrativen Services erfordern. In einigen Fällen ist es jedoch sinnvoll, mehrere administrative Unterteilungen einzurichten. Unterteilungen bieten sich insbesondere dann an, wenn Sie ein kleines Netzwerk mit Teilnetzen haben und das Netzwerk über einen größeren geographischen Bereich verteilt ist.

- **Haben Benutzer im Netzwerk ähnliche Anforderungen?**

  Eventuell haben Sie ein Netzwerk, das auf ein Gebäude beschränkt ist und nur eine relativ geringe Anzahl an Computern unterstützt. Diese Computer sind in verschiedene Teilnetzwerke aufgeteilt. Jedes Teilnetzwerk unterstützt Benutzergruppen mit verschiedenen Anforderungen. In diesem Beispiel können Sie für jedes Teilnetz eine administrative Unterteilung verwenden.

Planen der Router für Ihr Netzwerk

Sie werden sich erinnern, dass bei TCP/IP zwei Arten von Entitäten in einem Netzwerk vorhanden sind: Hosts und Router. Alle Netzwerke müssen Hosts enthalten, aber nicht alle Netzwerke erfordern Router. Die physikalische Topologie des Netzwerks bestimmt, ob Router erforderlich sind. In diesem Abschnitt werden Sie in die Konzepte der Netzwerktopologie und des Routings eingeführt. Diese Konzepte sind insbesondere dann wichtig, wenn Sie ein weiteres Netzwerk zu Ihrer vorhandenen Netzwerkumgebung hinzufügen möchten.

Hinweis – Ausführliche Details und Aufgaben zur Router-Konfiguration für IPv4-Netzwerke finden Sie unter „Paketweiterleitung und Routing bei IPv4-Netzwerken“ auf Seite 119. Ausführliche Details und Aufgaben zur Router-Konfiguration für IPv6-Netzwerke finden Sie unter „Konfiguration eines IPv6-Routers“ auf Seite 191.

Einführung in die Netzwerktopologie

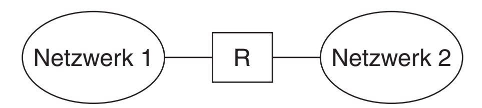
Die Netzwerktopologie beschreibt, wie Netzwerke aufgebaut sind. Router sind Entitäten, über die Netzwerke miteinander verbunden sind. Ein Router ist ein Computer, der über mindestens zwei Netzwerkschnittstellen verfügt und die IP-Weiterleitung implementiert. Ein System kann jedoch erst dann als Router arbeiten, nachdem es ordnungsgemäß konfiguriert wurde. Lesen Sie dazu die Beschreibung unter „Konfiguration eines IPv4-Routers“ auf Seite 126.

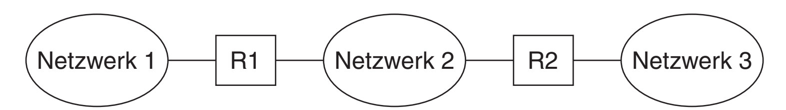
Router verbinden zwei oder mehr Netzwerke miteinander, um so größere Internetzwerke zu bilden. Die Router müssen so konfiguriert sein, dass sie Pakete zwischen zwei benachbarten Netzwerken übergeben. Außerdem müssen Router in der Lage sein, Pakete an Netzwerke weiterzuleiten, die hinter den benachbarten Netzwerken liegen.

In der folgenden Abbildung sind die grundlegenden Komponenten einer Netzwerktopologie gezeigt. Die erste Abbildung zeigt eine einfache Konfiguration mit zwei Netzwerken, die über

einen Router miteinander verbunden sind. Die zweite Abbildung zeigt eine Konfiguration mit drei Netzwerken, die über zwei Router miteinander kommunizieren. Im ersten Beispiel verbindet der Router R die Netzwerke 1 und 2 zu einem größeren Internetzwerk. Im zweiten·Beispiel verbindet der Router R1 die Netzwerke 1 und 2. Router R2 verbindet die Netzwerke 2 und 3. Diese Verbindungen bilden ein Netzwerk, das aus den Netzwerken 1, 2 und 3 besteht.

ABBILDUNG 2–3 Einfache Netzwerktopologie

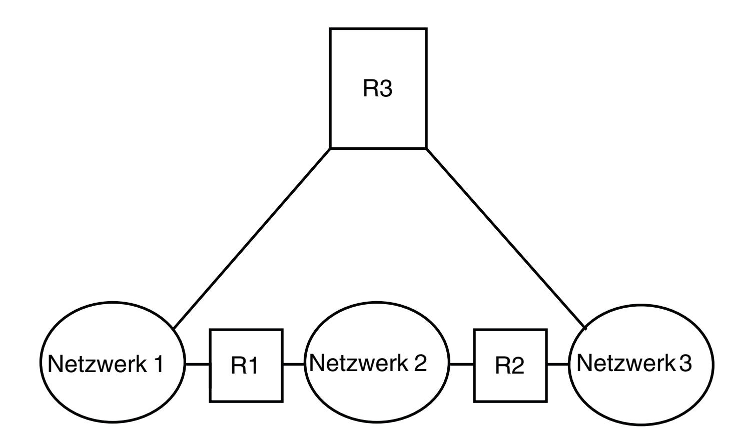




Neben dem Zusammenschließen von Netzwerken zu Internetzwerken haben Router die Aufgabe, Pakete zwischen Netzwerken weiterzuleiten, die auf den Adressen des Zielnetzwerks basieren. Je größer und komplexer Internetzwerke werden, desto mehr Entscheidungen muss jeder Router über die Paketziele treffen.

Die folgende Abbildung zeigt einen komplexeren Fall. Router R3 verbindet die Netzwerke 1 und 3 direkt. Diese Redundanz erhöht die Zuverlässigkeit. Wenn Netzwerk 2 ausfällt, stellt Router R3 immer noch eine Route zwischen den Netzwerken 1 und 3 bereit. Sie können viele Netzwerke miteinander verbinden. sie müssen jedoch die gleichen Netzwerkprotokolle verwenden.

ABBILDUNG 2–4 Eine Netzwerktopologie, die eine zusätzliche Route zwischen Netzwerken bereitstellt



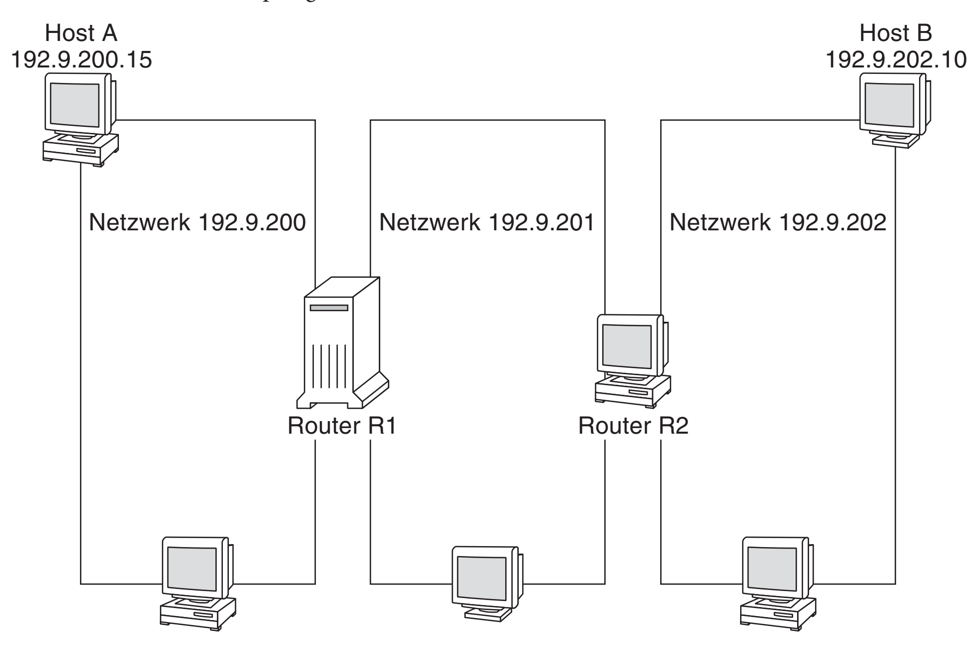
So übertragen Router Pakete

Die IP-Adresse des Empfängers, die einen Teil des Paket-Headers ist, legt fest, wie das Paket geleitet wird. Enthält diese Adresse die Netzwerknummer des lokalen Netzwerks, wird das Paket direkt an den Host mit dieser IP-Adresse geleitet. Stimmt die Netzwerknummer nicht mit der des lokalen Netzwerks über ein, wird das Paket an den Router des lokalen Netzwerks übergeben.

Router pflegen die Routing-Informationen in so genannten *Routing-Tabellen*. Diese Tabellen enthalten die IP-Adresse der Hosts und Router der Netzwerke, mit denen der Router verbunden ist. Darüber hinaus enthalten die Tabellen Verweise auf diese Netzwerke. Wenn ein Router ein Paket empfängt, prüft er seine Routing-Tabelle, um festzustellen, ob die im Header enthaltene Zieladresse in der Tabelle enthalten ist. Ist dies nicht der Fall, leitet der Router das Paket an einen anderen, in seiner Routing-Tabelle aufgeführten Router weiter. Weitere Informationen zu Routern finden Sie unter „Konfiguration eines IPv4-Routers“ auf Seite 126.

Die folgende Abbildung zeigt eine Netzwerktopologie mit drei Netzwerken, die über zwei Router miteinander verbunden sind.

ABBILDUNG 2–5 Netzwerktopologie mit drei miteinander verbundenen Netzwerken



Router R1 verbindet die Netzwerke `192.9.200` und `192.9.201`. Router R2 verbindet die Netzwerke `192.9.201` und `192.9.202`. Wenn Host A im Netzwerk `192.9.200` eine Nachricht an Host B im Netzwerk `192.9.202` sendet, treten die folgenden Ereignisse auf:

1. Host A sendet ein Paket über das Netzwerk `192.9.200`. Der Paket-Header enthält die IPv4-Adresse des Empfänger-Host B, `192.9.202.10` .
2. Kein Computer im Netzwerk `192.9.200` besitzt die IPv4-Adresse `192.9.202.10`. Aus diesem Grund akzeptiert Router R1 das Paket.
3. Router R1 prüft seine Routing-Tabellen. Kein Computer im Netzwerk `192.9.201` besitzt die Adresse `192.9.202.10`. Die Routing-Tabellen enthalten jedoch den Router R2.
4. R1 wählt daher R2 als „nächster Hop"-Router. R1 sendet das Paket an R2.
5. Da R2 das Netzwerk `192.9.201` mit `192.9.202` verbindet, besitzt R2 Routing-Informationen zu Host B. Router R2 leitet das Paket an das Netzwerk `192.9.202` weiter, in dem Host B das Paket schließlich akzeptiert.

Einführung in IPv6 (Überblick)

Dieses Kapitel bietet eine Übersicht zur Implementierung der Internet Protocol Version 6 (IPv6) in Oracle Solaris. Diese Implementierung umfasst den dazugehörigen Daemon sowie die Dienstprogramme, die den IPv6-Adressraum unterstützen.

IPv6- und IPv4-Adressen können in einer Oracle Solaris-Netzwerkumgebung gemeinsam existieren. Systeme, die mit IPv6-Adressen konfiguriert wurden, behalten auch ihre eventuell vorhandenen IPv4-Adressen. Vorgänge, die IPv6-Adressen betreffen, wirken sich nicht auf IPv4-Vorgänge aus und umgekehrt.

Folgende Themen werden behandelt:

- „Die wichtigsten Leistungsmerkmale von IPv6" auf Seite 74
- „Einführung in IPv6-Netzwerke" auf Seite 76
- „Einführung in die IPv6-Adressierung" auf Seite 78
- „Einführung in das IPv6 Neighbor Discovery-Protokoll" auf Seite 84
- „Automatische IPv6-Adresskonfiguration" auf Seite 86
- „Einführung in IPv6-Tunnel" auf Seite 87

Ausführliche Informationen zu IPv6 finden Sie in den folgenden Kapiteln.

- IPv6-Netzwerkplanung – Kapitel 4, „Planen eines IPv6-Netzwerks (Aufgaben)"
- IPv6-bezogene Aufgaben – Kapitel 7, „Konfigurieren eines IPv6-Netzwerks (Vorgehen)" und Kapitel 8, „Verwaltung eines TCP/IP-Netzwerks (Aufgaben)".
- IPv6-Details – Kapitel 11, „IPv6 im Detail (Referenz)"

Die wichtigsten Leistungsmerkmale von IPv6

Das wichtigste Leistungsmerkmal von IPv6 im Vergleich zu IPv4 ist der größere Adressraum. IPv6 verbessert also die Internetfähigkeiten in verschiedenen Bereichen. Dies wird in diesem Abschnitt ausführlicher beschrieben.

Erweiterte Adressierung

Die IP-Adressgröße ist von 32 Bit in IPv4 auf 128 Bit in IPv6 angestiegen, um mehr Ebenen der Adressierungshierarchie zu unterstützen. Darüber hinaus unterstützt IPv6 mehr adressierbare IPv6-Systeme. Weitere Informationen finden Sie unter „Einführung in die IPv6-Adressierung“ auf Seite 78.

Automatische Adresskonfiguration und Neighbor Discovery

Das *Neighbor Discovery (ND)*-Protokoll in IPv6 vereinfacht die automatische Konfiguration von IPv6-Adressen. Die *automatische Konfiguration* ist die Fähigkeit eines IPv6-Hosts, eine eigene IPv6-Adresse zu erzeugen, wodurch die Adressverwaltung einfacher und weniger zeitaufwändig wird. Weitere Informationen finden Sie unter „Automatische IPv6-Adresskonfiguration“ auf Seite 86.

Das Neighbor Discovery-Protokoll entspricht einer Kombination aus den folgenden IPv4-Protokollen: Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Router Discovery (RDISC) und ICMP Redirect. IPv6-Router verwenden das Neighbor Discovery-Protokoll zur Bekanntgabe des IPv6-Standortpräfix. IPv6-Hosts verwenden das Neighbor Discovery-Protokoll für verschiedene Zwecke, z. B. dem Anfordern des Präfix von einem IPv6-Router. Weitere Informationen finden Sie unter „Einführung in das IPv6 Neighbor Discovery-Protokoll“ auf Seite 84.

Vereinfachung des Header-Formats

Das IPv6-Header-Format wirft bestimmte Felder im IPv6-Header entweder ab oder macht sie optional. Durch diese Änderung werden die Bandbreitenkosten des IPv6-Header so niedrig wie möglich gehalten, ungeachtet der angewachsenen Adressgröße. Obwohl IPv6-Adressen viermal so lang wie IPv4-Adressen sind, ist der IPv6-Header nur doppelt so groß wie der IPv4-Header.

Verbesserte Unterstützung für IP-Header-Optionen

Änderungen an der Kodierung der IP-Header-Optionen ermöglichen eine effizientere Weiterleitung. Darüber hinaus ist die Längenbeschränkung von IPv6-Optionen weniger strikt. Diese Änderungen bieten größere Flexibilität bei der Einführung zukünftiger neuer Optionen.

Anwendungsunterstützung für IPv6-Adressierung

Viele wichtige Oracle Solaris-Netzwerkservices erkennen und unterstützen IPv6-Adressen, z. B.:

- Namen-Services wie DNS, LDAP und NIS. Weitere Informationen zur IPv6-Unterstützung durch diese Namen-Services finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .
- Anwendungen zur Authentifizierung und Durchsetzung der Privatsphäre, wie IP Security Architecture (IPsec) und Internet Key Exchange (IKE). Weitere Informationen finden Sie in Teil IV.
- Verschiedene Services, die vom IP Quality of Service (IPQoS) bereitgestellt werden. Weitere Informationen finden Sie in Teil VII.
- Failover-Erkennung, wie sie von IP Network Multipathing (IPMP) bereitgestellt wird. Weitere Informationen finden Sie in Teil VI.

Weitere IPv6-Ressourcen

Zusätzlich zu den Angaben in diesem Teil des Handbuchs finden Sie Informationen zu IPv6 in den im Folgenden aufgeführten Quellen.

IPv6 Requests for Comments und Internet Drafts

Zu IPv6 sind zahlreiche RFCs verfügbar. In der folgenden Tabelle sind die wichtigsten IPv6-Artikel und deren Internet Engineering Task Force (IETF)-Web-Speicherorte zum Zeitpunkt der Drucklegung dieser Dokumentation aufgeführt.

TABELLE 3–1 IPv6–bezogene RFCs und Internet Drafts

RFC oder Internet Draft	Thema	Zu finden in:
RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*	Beschreibt die Leistungsmerkmale und Funktionen des IPv6 Neighbor Discovery-Protokolls.	http://www.ietf.org/rfc/rfc2461.txt$number=2461 (`http://www.ietf.org/rfc/rfc2461.txt?number-2461`)

TABELLE 3–1 IPv6–bezogene RFCs und Internet Drafts *(Fortsetzung)*

RFC oder Internet Draft	Thema	Zu finden in:
RFC 3306, *Unicast—Prefix—Based IPv6 Multicast Addresses*	Beschreibt das Format und die Typen von IPv6-Multicast-Adressen.	ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt (`ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt`)
RFC 3484: *Default Address Selection for Internet Protocol version 6 (IPv6)*	Beschreibt die bei der standardmäßigen IPv6-Adressauswahl verwendeten Algorithmen.	http://www.ietf.org/rfc/rfc3484?number=3484 (`http://www.ietf.org/rfc/rfc3484.txt?number=3484`)
RFC 3513, *Internet Protocol version 6 (IPv6) Addressing Architecture*	Enthält vollständige Informationen zu den IPv6-Adresstypen sowie zahlreiche Beispiele.	http://www.ietf.org/rfc/rfc3513.txt?number=3513 (`http://www.ietf.org/rfc/rfc3513.txt?number=3513`)
RFC 3587, *IPv6 Global Unicast Address Format*	Definiert das Standardformat für IPv6-Unicast-Adressen.	http://www.ietf.org/rfc/rfc3587.txt?number=3587 (`http://www.ietf.org/rfc/rfc3587.txt?number=3587`)

Websites

Die folgenden Websites enthalten nützliche Informationen zu IPv6.

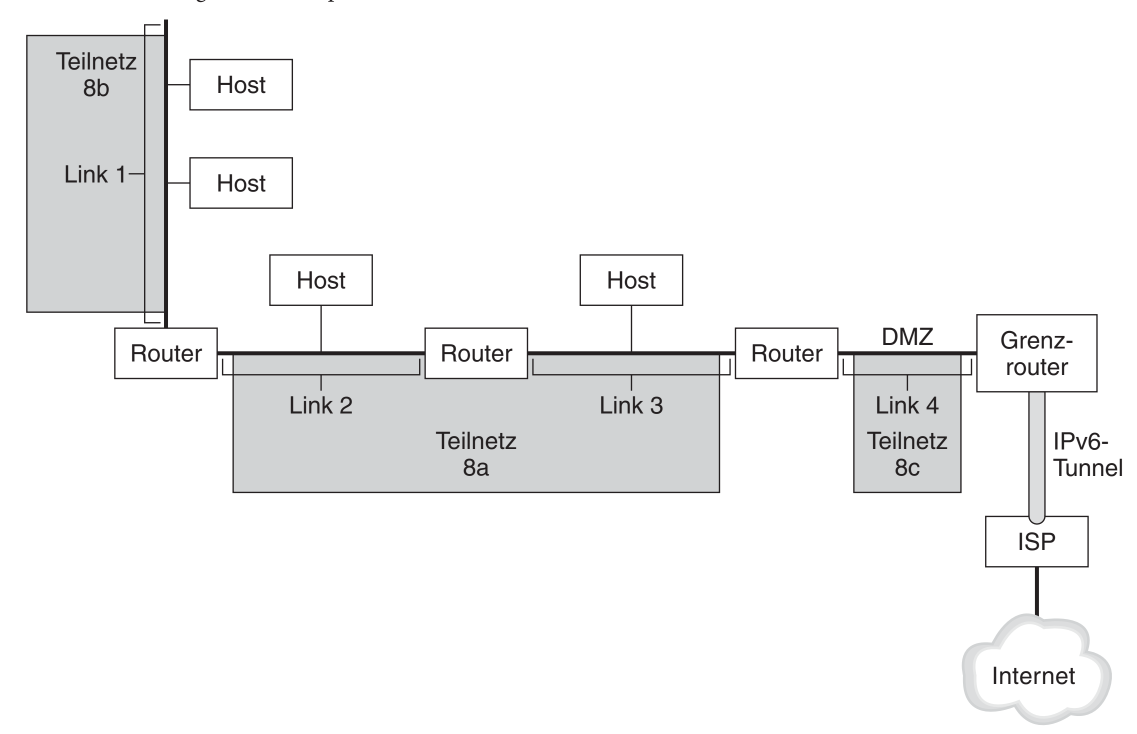
TABELLE 3–2 IPv6–bezogene Websites

Website	Beschreibung	Zu finden in:
IPv6-Forum	Links zu IPv6-bezogenen Präsentationen, Ereignissen, Klassen und weltweiten Implementationen können von der Website dieser Organisation aufgerufen werden.	http://www.ipv6forum.com
Internet Educational Task Force IPv6 Working Group	Links zu allen wichtigen IPv6 RFCs und Internet Drafts finden Sie auf der Startseite dieser IETF-Arbeitsgruppe.	http://www.ietf.org/html.charters/ipv6-charter.html

Einführung in IPv6-Netzwerke

Dieser Abschnitt enthält eine Einführung in die wichtigsten Begriffe einer IPv6-Netzwerktopologie. Die folgende Abbildung zeigt die allgemeinen Komponenten eines IPv6-Netzwerks.

ABBILDUNG 3–1 Allgemeine Komponenten eines IPv6-Netzwerks



Die Abbildung zeigt ein IPv6-Netzwerk sowie dessen Verbindungen mit einem ISP. Das interne Netzwerk besteht aus den Links 1, 2, 3 und 4. Jeder Link wird aus Hosts gebildet und von einem Router abgeschlossen. Link 4, die DMZ des Netzwerks, wird an einem Ende durch den Grenzrouter terminiert. Der Grenzrouter führt einen IPv6-Tunnel zu einem ISP aus, der den Internetanschluss für das Netzwerk herstellt. Links 2 und 3 werden als Teilnetz 8a verwaltet. Teilnetz 8b besteht nur aus Systemen von Link 1. Teilnetz 8c ist hängt mit dem DMZ auf Link 4 zusammen.

Wie Abbildung 3–1 zeigt, weist ein IPv6-Netzwerk im Wesentlichen die gleichen Komponenten wie ein IPv4-Netzwerk auf. Dennoch unterscheidet sich die IPv6-Terminologie etwas von der IPv4-Terminologie. Im Folgenden ist eine Liste der gebräuchlichsten Begriffe für Netzwerkkomponenten aufgeführt, die in einem IPv6-Kontext verwendet werden.

Knoten Ein System mit einer IPv6-Adresse und einer Schnittstelle, die zur Unterstützung von IPv6 konfiguriert wurde. Dieser generische Begriff gilt sowohl für Hosts als auch für Router.

IPv6-Router Ein Knoten, der IPv6-Pakete weiterleitet. Mindestens eine der Router-Schnittstellen muss zur Unterstützung von IPv6 konfiguriert sein. Ein IPv6-Router kann auch den registrierten IPv6-Standortpräfix des Unternehmens über das interne Netzwerk bekannt geben.

IPv6-Host Ein Knoten mit einer IPv6-Adresse. Ein IPv6-Host kann mehrere Schnittstellen besitzen, die zur Unterstützung von IPv6 konfiguriert wurden. Wie in IPv4-Netzwerken leiten IPv6-Hosts keine Pakete weiter.

Link Ein einzelnes, zusammenhängendes Netzwerkmedium, das mit einem Ende an einen Router angeschlossen ist.

Neighbor Ein IPv6-Knoten, der sich auf dem gleichen Link wie der lokale Knoten befindet.

IPv6-Teilnetz Das administrative Segment eines IPv6-Netzwerks. Komponenten eines IPv6-Teilnetzes können, wie bei IPv4, direkt mit allen Knoten auf einem Link kommunizieren. Knoten auf einem Link können, falls erforderlich, in separaten Teilnetzen verwaltet werden. Darüber hinaus unterstützt IPv6 Multilink-Teilnetze, in denen die Knoten auf mehreren Links Komponenten eines einzelnen Teilnetzes sein können. Links 2 und 3 in Abbildung 3–1 sind z. B. Komponenten des Multilink-Teilnetzes 8a.

IPv6-Tunnel Ein Tunnel, der einen virtuellen Punkt-zu-Punkt-Pfad zwischen einem IPv6-Knoten und einem anderen IPv6-Knotenendpunkt darstellt. IPv6 unterstützt manuell konfigurierbare Tunnel und automatische 6to4-Tunnel.

Grenzrouter Der Router an einem Ende eines Netzwerks, der ein Ende eines IPv6-Tunnels für einen Endpunkt außerhalb des lokalen Netzwerks darstellt. Dieser Router muss über mindestens eine IPv6-Schnittstelle mit dem internen Netzwerk verfügen. Für das externe Netzwerk kann der Router über eine IPv6-Schnittstelle oder eine IPv4-Schnittstelle verfügen.

Einführung in die IPv6-Adressierung

IPv6-Adressen werden Schnittstellen anstelle von Knoten zugewiesen, da Knoten über mehrere Schnittstellen verfügen können. Sie können einer Schnittstelle jedoch mehrere IPv6-Adressen zuweisen.

Hinweis – Vollständige technische Informationen zum IPv6-Adressenformat finden Sie in RFC 2374, IPv6 Global Unicast Address Format (`http://www.ietf.org/rfc/rfc2374.txt?number=2374`)

IPv6 definiert drei Adresstypen:

Unicast Bezieht sich auf eine Schnittstelle auf einem einzelnen Knoten.

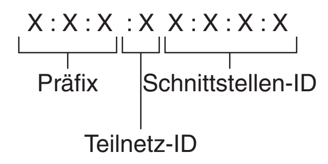
Multicast Bezieht sich auf eine Gruppe von Schnittstellen, in der Regel auf verschiedenen Knoten. Pakete, die eine Multicast-Adresse gesendet werden, werden an alle Mitglieder der *Multicast-Gruppe* geleitet.

Anycast Bezieht sich auf eine Gruppe von Schnittstellen, in der Regel auf verschiedenen Knoten. Pakete, die an eine Anycast-Adresse gesendet werden, gehen an den Mitgliedsknoten der *Anycast-Gruppe*, der dem Absender am nähesten ist.

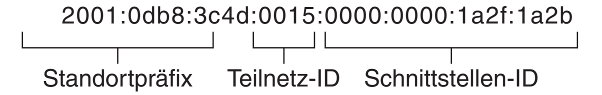
Komponenten einer IPv6-Adresse

Eine IPv6-Adresse ist 128 Bit lang und besteht aus acht 16-Bit-Feldern, die durch Doppelpunkte voneinander getrennt sind. Jedes Feld muss eine hexadezimale Zahl enthalten, im Gegensatz zur getrennten dezimale Notation von IPv4-Adressen. In der folgenden Abbildung stellen die „x" hexadezimale Zahlen dar.

ABBILDUNG 3–2 Allgemeines IPv6-Adressformat



Beispiel



Die drei Felder auf der linken Seite (48 Bit) enthalten das *Standortpräfix*. Das Präfix beschreibt die *öffentliche Topologie*, die Ihrem Standort normalerweise von einem ISP oder einer Regional Internet Registry (RIR) zugewiesen wird.

Das nächste Feld ist die 16-Bit-*Teilnetz-ID*, die Sie (oder ein anderer Administrator) Ihrem Standort zugewiesen haben. Die Teilnetz-ID beschreibt die *private Topologie*, die auch als *Standorttopologie* bezeichnet wird, da sie nur für Ihren Standort gilt.

Die höherwertigsten vier Felder (64 Bit) enthalten die *Schnittstellen-ID*, die auch als *Token* bezeichnet wird. Die Schnittstellen-ID wird entweder automatisch von der MAC-Adresse der Schnittstelle oder manuell im EUI-64-Format konfiguriert.

Betrachten Sie noch einmal die Adresse aus Abbildung 3–2:

```
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
```

In diesem Beispiel werden alle 128 Bit einer IPv6-Adresse gezeigt. Die ersten 48 Bit (`2001:0db8:3c4d`) enthalten das Standortpräfix, das die öffentliche Topologie darstellt. Die nächsten 16 Bit (`0015`) enthalten die Teilnetz-ID, die die private Topologie des Standorts darstellt. Die nachrangigen rechten 64 Bit (`0000:0000:1a2f:1a2b`) enthalten die Schnittstellen-ID.

Abkürzen von IPv6-Adressen

Die meisten IPv6-Adressen belegen nicht alle verfügbaren 128 Bit. Dies führt zu Feldern, die entweder mit Nullen aufgefüllt werden oder nur Nullen enthalten.

Die IPv6-Adressierungsarchitektur ermöglicht Ihnen eine Notation mit zwei Doppelpunkten (: :), um zusammenhängende 16-Bit-Felder mit Nullen darzustellen. So können Sie die IPv6-Adresse aus Abbildung 3–2 beispielsweise schreiben, indem Sie die zwei zusammenhängenden Felder mit Nullen in der Schnittstellen-ID durch zwei Doppelpunkte ersetzen. Die resultierende Adresse lautet dann `2001:0db8:3c4d:0015::1a2f:1a2b`. Andere aus Null bestehende Felder können als einzelne 0 dargestellt werden. Sie können führende Nullen in einem Feld weglassen, d. h. `0db8` kann beispielsweise als `db8` geschrieben werden.

Die Adresse `2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b` kann also zu `2001:db8:3c4d:15::1a2f:1a2b` verkürzt werden.

Sie können die Notation mit zwei Doppelpunkten verwenden, um alle zusammenhängenden Felder mit Nullen in der IPv6-Adresse zu ersetzen. So kann die IPv6-Adresse `2001:0db8:3c4d:0015:0000:d234::3eee:0000` zu `2001:db8:3c4d:15:0:d234:3eee::` verkürzt werden.

Präfixe in IPv6

Die linken Felder der IPv6-Adresse enthalten das zum Routen von IPv6-Paketen verwendete Präfix. IPv6-Präfixe weisen das folgende Format auf:

Präfix/*Länge in Bit*

Die Präfixlänge wird in der Classless Inter-Domain Routing (CIDR)-Notation angegeben. Die CIDR-Notation wird durch einen Schrägstrich am Ende der Adresse gekennzeichnet, dem die Präfixlänge in Bit folgt. Weitere Informationen zu IP-Adressen im CIDR-Format finden Sie unter „Erstellen eines CIDR IPv4-Adressierungsschemas“ auf Seite 64.

Das *Standortpräfix* einer IPv6-Adresse belegt bis zu 48 der linken Bit einer IPv6-Adresse. Beispielsweise umfasst das Standortpräfix der IPv6-Adresse

`2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48` 48 Bit auf der linken Seite: `2001:db8:3c4d`. Sie verwenden die folgende Notation mit komprimierten Nullen, um dieses Präfix darzustellen:

```
2001:db8:3c4d::/48
```

Hinweis – Das Präfix `2001:db8::/32` wird speziell für Dokumentationsbeispiele verwendet.

Sie können auch ein *Teilnetzpräfix* angeben, das die interne Netzwerktopologie für einen Router definiert. Die IPv6-Beispieladresse hat das folgende Teilnetzpräfix.

```
2001:db8:3c4d:15::/64
```

Das Teilnetzpräfix umfasst immer 64 Bit. Diese Bit umfassen 48 Bit für das Standortpräfix, zusätzlich zu den 16 Bit für die Teilnetz-ID.

Die folgenden Präfixe wurden für besondere Zwecke reserviert:

`2002::/16` Gibt an, dass ein 6to4-Routing-Präfix folgt.

`fe80::/10` Gibt an, dass eine Link-lokale Adresse folgt.

`ff00::/8` Gibt an, dass eine Multicast-Adresse folgt.

Unicast-Adressen

IPv6 umfasst zwei unterschiedliche Unicast-Adresszuweisungen:

- Globale Unicast-Adresse
- Link-lokale Adresse

Der Typ einer Unicast-Adresse wird durch die linken (hochrangigen) Bit in der Adresse festgelegt, die das Präfix enthalten.

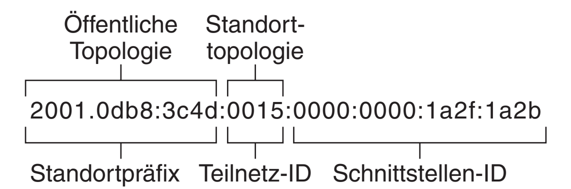
Die Unicast-Adresse ist in der folgenden Hierarchie strukturiert:

- Öffentliche Topologie
- Standorttopologie (privat)
- Schnittstellen-ID

Globale Unicast-Adresse

Die globale Unicast-Adresse ist weltweit einmalig im Internet. Die unter „Präfixe in IPv6“ auf Seite 80 gezeigte IPv6-Beispieladresse ist eine globale Unicast-Adresse. Die folgende Abbildung zeigt den Umfang der globalen Unicast-Adresse im Vergleich zu Komponenten der IPv6-Adresse.

ABBILDUNG 3–3 Komponenten der globalen Unicast-Adresse



Öffentliche Topologie

Das Standortpräfix legt die *öffentliche Topologie* Ihres Netzwerks gegenüber einem Router fest. Sie beziehen das Standortpräfix für Ihr Unternehmen von einem ISP oder der Regional Internet Registry (RIR).

Standorttopologie und IPv6-Teilnetze

In IPv6 definiert die *Teilnetz-ID* ein administratives Teilnetz des Netzwerks und umfasst bis zu 16 Bit. Sie weisen die Teilnetz-ID während der Konfiguration eines IPv6-Netzwerks zu. Das *Teilnetzpräfix* legt die Standorttopologie für einen Router fest, indem es den Link angibt, dem das Teilnetz zugewiesen wurde.

IPv6-Teilnetze gleichen konzeptuell IPv4-Teilnetzen, da jedes Teilnetz in der Regel einem Hardware-Link zugewiesen ist. IPv6-Teilnetz-IDs werden jedoch in hexadezimaler Notation, IPv4-Teilnetz-IDs hingegen in getrennter dezimaler Notation ausgedrückt.

Schnittstellen-ID

Die *Schnittstellen-ID* gibt eine Schnittstelle für einen bestimmten Knoten an. Eine Schnittstellen-ID muss innerhalb des Teilnetzes einmalig sein. IPv6-Hosts können das Neighbor Discovery-Protokoll verwenden, um eigene Schnittstellen-IDs automatisch zu erzeugen. Neighbor Discovery generiert basierend auf der MAC- oder der EUI-64-Adresse der Host-Schnittstelle automatisch die Schnittstellen-ID. Sie können Schnittstellen-IDs auch manuell zuweisen. Dies wird für IPv6-Router und IPv6-konforme Server empfohlen. Eine Anleitung zum manuellen Erstellen einer EUI-64-Adresse finden Sie in RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture.

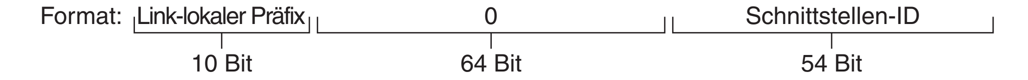
Globale Unicast-Übergangsadressen

Als Übergangslösung bietet das IPv6-Protokoll die Möglichkeit, eine IPv4-Adresse in eine IPv6-Adresse einzubetten. Dieser IPv4-Adresstyp vereinfacht das Tunneling von IPv6-Paketen über vorhandene IPv4-Netzwerke. Ein Beispiel einer globalen Unicast-Übergangsadresse ist die 6to4-Adresse. Weitere Informationen zur 6to4-Adressierung finden Sie unter „Automatische 6to4-Tunnel“ auf Seite 312.

Link-lokale Unicast-Adresse

Die Link-lokale Unicast-Adresse kann nur auf dem lokalen Netzwerklink verwendet werden. Link-lokale Adressen sind außerhalb des Unternehmens ungültig und werden nicht erkannt. Das folgende Beispiel zeigt das Format einer Link-lokalen Adresse.

BEISPIEL 3–1 Komponenten der Link-lokalen Unicast-Adresse



Beispiel: fe80::123e:456d

Ein *Link-lokaler Präfix* hat das folgende Format:

`fe80::`*Schnittstellen-ID*`/10`

Das Folgende ist ein Beispiel einer Link-lokalen Adresse:

`fe80::23a1:b152`

`fe80` — Hexadezimale Darstellung des binären 10-Bit-Präfixes 1111111010. Dieses Präfix identifiziert den Typ der IPv6-Adresse als Link-lokal.

Schnittstellen-ID — Hexadezimale Adresse der Schnittstelle, die in der Regel von der 48-Bit-MAC-Adresse abgeleitet wird.

Wenn Sie IPv6 während der Oracle Solaris-Installation aktivieren, wird die Schnittstelle mit der niedrigsten Nummer auf dem lokalen Computer mit einer Link-lokalen Adresse konfiguriert. Jede Schnittstelle benötigt mindestens eine Link-lokale Adresse, um den Knoten gegenüber anderen Knoten auf dem lokalen Link zu identifizieren. Aus diesem Grund müssen Sie die Link-lokalen Adressen zusätzlicher Schnittstellen eines Knotens manuell konfigurieren. Nach der Konfiguration verwendet der Knoten die Link-lokalen Adressen zur automatischen Adresskonfiguration und für das Neighbor Discovery-Protokoll.

Multicast-Adressen

IPv6 unterstützt die Verwendung von Multicast-Adressen. Die Multicast-Adresse gibt eine *Multicast-Gruppe* an, eine Gruppe von Schnittstellen, die sich in der Regel auf verschiedenen Knoten befinden. Eine Schnittstelle kann mehreren Multicast-Gruppen angehören. Lauten die ersten 16 Bit einer IPv6-Adresse `ff00` *n*, so handelt es sich bei der Adresse um eine Multicast-Adresse.

Multicast-Adressen werden für das Senden von Informationen oder Services an alle Schnittstellen verwendet, die zu einer Multicast-Gruppe gehören. Beispielsweise kann durch einmaliges Verwenden von Multicast-Adressen mit allen IPv6-Knoten auf dem lokalen Link kommuniziert werden.

Wenn die IPv6-Unicast-Adresse einer Schnittstelle erstellt wird, macht der Kernel die Schnittstelle automatisch zu einem Mitglied bestimmter Multicast-Gruppen. Beispielsweise macht der Kernel jeden Knoten zu einem Mitglied der Multicast-Gruppe „Angeforderter KnotenNode", die vom Neighbor Discovery-Protokoll zur Erkennung der Erreichbarkeit verwendet wird. Darüber hinaus macht der Kernel einen Knoten automatisch zu einem Mitglied der Multicast-Gruppen „Alle Knoten" oder „Alle Router".

Ausführliche Informationen zur Multicast-Adressen finden Sie unter „IPv6-Multicast-Adressen im Detail" auf Seite 280. Technische Informationen finden Sie in RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses (`ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt`), in der das Multicast-Adressenformat erläutert wird. Weitere Informationen zur ordnungsgemäßen Verwendung von Multicast-Adressen und -Gruppen finden Sie in RFC 3307, Allocation Guidelines for IPv6 Multicast Addresses (`ftp://ftp.rfc-editor.org/in-notes/rfc3307.txt`).

Anycast-Adressen und -gruppen

IPv6-Anycast-Adressen geben eine Schnittstellengruppe an, die sich auf unterschiedlichen IPv6-Knoten befindet. Jede Schnittstellengruppe wird als eine *Anycast-Gruppe bezeichnet*. Wenn ein Paket an eine Anycast-Adresse gesendet wird, empfängt das Anycast-Gruppenmitglied das Paket, das dem Sender am nächsten ist.

Hinweis – Das Erstellen von Anycast-Adressen und -Gruppen wird in Oracle Solaris nicht unterstützt. Jedoch können Oracle Solaris IPv6-Knoten Pakete an Anycast-Adressen senden. Weitere Informationen finden Sie unter „Sicherheitsbetrachtungen bei Tunneln zu einem 6to4-Relay-Router" auf Seite 314.

Einführung in das IPv6 Neighbor Discovery-Protokoll

IPv6 führt das Neighbor Discovery-Protokoll ein, das die Interaktion zwischen benachbarten Knoten über das Messaging abzuwickelt. *Benachbarte (Neighbor) Knoten* sind IPv6-Knoten, die sich auf dem gleichen Link befinden. So kann ein Knoten durch das Senden von Neighbor Discovery-Nachrichten die Link-lokale Adresse eines benachbarten Knotens in Erfahrung bringen. Das Neighbor Discovery-Protokoll steuert die folgenden wichtigen Aktivitäten auf dem lokalen IPv6-Link:

- **Router-Erkennung** – Unterstützt Hosts beim Lokalisieren von Routern auf dem lokalen Link.
- **Automatische Adresskonfiguration** – Ermöglicht es einem Knoten, die IPv6-Adressen für die eigenen Schnittstellen automatisch zu konfigurieren.
- **Präfix-Erkennung** – Ermöglicht es Knoten, die einem Link zugewiesenen, bekannten Teilnetzpräfixe zu erkennen. Knoten verwenden Präfixe, um Ziele auf dem lokalen Link von Zielen zu unterscheiden, die nur über einen Router erreicht werden können.
- **Adressauflösung** – Hilft Knoten beim Feststellen der Link-lokalen Adresse eines benachbarten Knotens, vorausgesetzt, es ist nur die IP-Adresse des Ziels vorhanden.
- **Ermittelung des nächsten Hop** – Verwendet einen Algorithmus zur Ermittlung der IP-Adresse eines Paketempfängers, der sich einen Hop über den lokalen Link hinaus befindet. Der nächste Hop kann ein Router oder der Zielknoten sein.
- **Neighbor-Unerreichbarkeitserkennung** – Hilft Knoten festzustellen, ob ein benachbarter Knoten noch immer erreichbar ist. Bei Routern und Hosts kann die Adressauflösung wiederholt werden.
- **Erkennung doppelt vorhandener Adressen** – Ermöglicht es einem Knoten festzustellen, ob eine von einem Knoten gewünschte Adresse bereits von einem anderen Knoten verwendet wird.
- **Umleitung** – Ermöglicht es einem Router, einen Host über einen Knoten im ersten Hop zu informieren, über den ein bestimmtes Ziel besser erreicht werden kann.

Das Neighbor Discovery-Protokoll verwendet den folgenden ICMP-Nachrichtentyp zur Kommunikation unter den Knoten auf einem Link:

- Router Solicitation-Nachrichten
- Router Advertisement-Nachrichten
- Neighbor Solicitation-Nachrichten
- Neighbor Advertisement-Nachrichten
- Umleitung

Ausführliche Informationen zu den Neighbor Discovery-Nachrichten und andere Themen zum Neighbor Discovery-Protokoll finden Sie unter „IPv6 Neighbor Discovery-Protokoll“ auf Seite 299. Technische Informationen zu Neighbor Discovery finden Sie in RFC 2461, Neighbor Discovery for IP Version 6 (IPv6) (`http://www.ietf.org/rfc/rfc2461.txt?number=2461`).

Automatische IPv6-Adresskonfiguration

Eine wichtige Funktion von IPv6 ist die Fähigkeit des Hosts, eine Schnittstelle automatisch zu konfigurieren. Über das Neighbor Discovery-Protokoll lokalisiert der Host einen IPv6-Router auf dem lokalen Link und fordert einen Standortpräfix an. Bei einer automatischen Konfiguration führt der Host Folgendes aus:

- Er erstellt eine Link-lokale Adresse für jede Schnittstelle, die keinen Router auf dem Link benötigt.
- Er prüft die Einmaligkeit der Adresse auf dem Link, die keinen Router auf dem Link benötigt.
- Er legt fest, ob die globalen Adressen über einen statusfreien Mechanismus, einen statusbehafteter Mechanismus oder über beide Mechanismen bezogen werden. (Erfordert einen Router auf dem Link.)

Einführung in die statusfreie automatische Konfiguration

Die statusfreie automatische Konfiguration erfordert keine manuelle Konfiguration der Hosts, eine minimale Konfiguration der Router (wenn überhaupt) und keine zusätzlichen Server. Mit dem statusfreien Mechanismus kann ein Host eigene Adressen generieren. Dazu verwendet der statusfreie Mechanismus lokale Informationen sowie über Router bekannt gegebene nicht-lokale Informationen.

Sie können temporäre Adressen für eine Schnittstelle implementieren, die ebenfalls automatisch konfiguriert werden. Sie aktivieren einen temporären Adresstoken für eine oder mehrere Schnittstellen auf einem Host. Im Gegensatz zu standardmäßigen, automatisch konfigurierten IPv6-Adressen besteht eine temporäre Adresse aus dem Standortpräfix und einer zufällig erzeugten 64-Bit-Zahl. Diese Zufallszahl wird zur Schnittstellen-ID der IPv6-Adresse. Mit einer temporären Adresse als Schnittstellen-ID wird keine Link-lokale Adresse erzeugt.

Router geben alle Präfixe bekannt, die auf diesem Link zugewiesen wurden. IPv6-Hosts verwenden die Neighbor Discovery, um einen Teilnetzpräfix von einem lokalen Router zu beziehen. Hosts erstellen automatisch IPv6-Adressen, indem sie das Teilnetzpräfix mit einer Schnittstellen-ID kombinieren, die von der MAC-Adresse einer Schnittstelle erzeugt wird. Wenn keine Router vorhanden sind, kann ein Host nur Link-lokale Adressen erzeugen. Link-lokale Adressen können nur für die Kommunikation mit Knoten auf dem gleichen Link verwendet werden.

Hinweis – Verwenden Sie keine statusfreie automatische Konfiguration, um IPv6-Adressen von Servern zu erstellen. Hosts erzeugen automatisch Schnittstellen-IDs, die auf Hardware-spezifischen Informationen während der automatischen Konfiguration beruhen. Die aktuelle Schnittstellen-ID könnte ungültig werden, wenn die vorhandene Schnittstelle gegen eine neue ausgetauscht wird.

Einführung in IPv6-Tunnel

Bei den meisten Unternehmen muss die Einführung von IPv6 in einem bestehenden IPv4-Netzwerk allmählich und schnittweise erfolgen. Die Oracle Solaris-Dual-Stack-Umgebung unterstützt sowohl IPv4 als auch IPv6. Da die meisten Netzwerke das IPv4-Protokoll verwenden, sind für IPv6-Netzwerke derzeit besondere Vorkehrungen erforderlich, um außerhalb ihrer Grenzen kommunizieren zu können. Zu diesem Zweck setzen IPv6-Netzwerke Tunnel ein.

Bei den meisten IPv6-Tunnelszenarios wird das abgehende IPv6-Paket in ein IPv4-Paket gekapselt. Der Grenzrouter des IPv6-Netzwerks richtet einen Punkt-zu-Punkt-Tunnel über die IPv4-Netzwerke zu einem Grenzrouter im IPv6-Zielnetzwerk ein. Das Paket durchläuft den Tunnel zum Grenzrouter im Zielnetzwerk, der das Paket entkapselt. Dann leitet der Router das separate IPv6-Paket an den Zielknoten weiter.

Die Oracle Solaris-Implementation von IPv6 unterstützt die folgenden Tunneling-Szenarios:

- Ein manuell konfigurierter Tunnel zwischen zwei IPv6-Netzwerken über ein IPv4-Netzwerk. Das IPv4-Netzwerk kann das Internet oder ein lokales Netzwerk innerhalb eines Unternehmens sein.
- Ein manuell konfigurierter Tunnel zwischen zwei IPv4-Netzwerken über ein IPv6-Netzwerk, in der Regel innerhalb eines Unternehmens.
- Ein dynamisch konfigurierter, automatischer 6to4-Tunnel zwischen zwei IPv6-Netzwerken über ein IPv4-Netzwerk bei einem Unternehmen oder über das Internet.

Ausführliche Informationen zu IPv6-Tunneln finden Sie unter „IPv6-Tunnel“ auf Seite 308. Weitere Informationen zu IPv4-zu-IPv4-Tunneln und VPN finden Sie unter „Virtuelle private Netzwerke und IPsec“ auf Seite 527.

KAPITEL 4

Planen eines IPv6-Netzwerks (Aufgaben)

Die Bereitstellung von IPv6 in einem neuen oder einem vorhandenen Netzwerk erfordert einen erheblichen Planungsaufwand. In diesem Kapitel werden die zur Planung erforderlichen Schritte beschrieben. Diese Schritte sind notwendig, um IPv6 an Ihrem Standort zu konfigurieren. Bei vorhandenen Netzwerken sollte die Bereitstellung von IPv6 schrittweise vorgenommen werden. Die Themen in diesem Kapitel unterstützen Sie dabei, IPv6 phasenweise in ein anderweitig IPv4-basiertes Netzwerk einzuführen.

In diesem Kapitel werden folgende Themen behandelt:

- „Planung der Einführung von IPv6 (Übersicht der Schritte)“ auf Seite 89
- „Szenario einer IPv6-Netzwerktopologie“ auf Seite 91
- „Vorbereiten eines bestehenden Netzwerks zur Unterstützung von IPv6“ auf Seite 93
- „Vorbereiten eines IPv6-Adressierungsplans“ auf Seite 98

Eine Einführung in die Konzepte von IPv6 finden Sie in Kapitel 3, „Einführung in IPv6 (Überblick)“. Ausführliche Informationen zu IPv6 finden Sie in Kapitel 11, „IPv6 im Detail (Referenz)“.

Planung der Einführung von IPv6 (Übersicht der Schritte)

Führen Sie die in der folgenden Tabelle aufgeführten Aufgaben nacheinander durch, um die zur Einführung von IPv6 erforderlichen Planungsaufgaben erfolgreich abzuschließen.

In der folgenden Tabelle sind verschiedene Aufgaben beschrieben, die zum Konfigurieren des IPv6-Netzwerks erforderlich sind. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
1. Vorbereiten Ihrer Hardware zur Unterstützung von IPv6.	Stellen Sie sicher, dass Ihre Hardware zur Unterstützung von IPv6 aufgerüstet werden kann.	„Vorbereiten der Netzwerktopologie auf die Unterstützung von IPv6“ auf Seite 93
2. Einen ISP beauftragen, der IPv6 unterstützt.	Stellen Sie sicher, dass Ihr aktueller ISP IPv6 unterstützt. Wenden Sie sich andernfalls an einen ISP, der IPv6 unterstützt. Sie können zwei ISP verwenden, einen für IPv6- und einen für IPv4-Kommunikationen.	
3. Sicherstellen, dass Ihre Anwendungen IPv6-konform sind.	Überprüfen Sie, ob Ihre Anwendungen in einer IPv6-Umgebung ausgeführt werden können.	„So bereiten Sie Netzwerkservices auf die Unterstützung von IPv6 vor“ auf Seite 95
4. Beziehen eines Standortpräfix.	Beziehen Sie einen 48-Bit-Standortpräfix für Ihren Standort von Ihrem ISP oder dem nächsten RIR.	„Beziehen eines Standortpräfix“ auf Seite 98
5. Erstellen eines Teilnetz-Adressierungsplans.	Bevor Sie IPv6 auf den verschiedenen Knoten in Ihrem Netzwerk konfigurieren können, müssen Sie die allgemeine IPv6-Netzwerktopologie und das Adressierungsschema planen.	„Erstellen eine Nummerierungsschemas für Teilnetze“ auf Seite 98
6. Entwerfen eines Plans für die Nutzung von Tunneln.	Legen Sie fest, welche Router Tunnel zu anderen Teilnetzen oder externen Netzwerken ausführen sollen.	„Planung für Tunnel in der Netzwerktopologie“ auf Seite 96
7. Erstellen eines Adressierungsplans für Entitäten im Netzwerk.	Setzen Sie Ihren Plan zur Adressierung von Servern, Routern und Hosts vor der IPv6-Konfiguration um.	„Erstellen eines IPv6-Adressierungsplans für Knoten“ auf Seite 99
8. Entwickeln einer IPv6-Sicherheitsrichtlinie.	Berücksichtigen Sie bei der Entwicklung einer IPv6-Sicherheitsrichtlinie IP Filter, IP-Sicherheitsarchitektur (IPsec), Internet Key Exchange (IKE) und andere Oracle Solaris-Sicherheitsfunktionen.	Teil IV
9. (Optional) Einrichten einer DMZ.	Aus Sicherheitsgründen benötigen Sie einen Adressierungsplan für die DMZ und die darin enthaltenen Entitäten, bevor Sie IPv6 konfigurieren.	„Sicherheitsbetrachtungen bei der Einführung von IPv6“ auf Seite 97
10. Aktivieren der Knoten zur Unterstützung von IPv6.	Konfigurieren Sie IPv6 auf allen Routern und Hosts.	„Konfiguration eines IPv6-Routers (Übersicht der Schritte)“ auf Seite 191
11. Aktivieren der Netzwerkservices.	Stellen Sie sicher, dass bereits vorhandene Server IPv6 unterstützen können.	„Aufgaben bei der Verwaltung von TCP/IP Netzwerken (Übersicht der Schritte)“ auf Seite 220

Aufgabe	Beschreibung	Siehe
12. Aktualisieren der Namen-Server zur Unterstützung von IPv6.	Stellen Sie sicher, dass die DNS-, NIS- und LDAP-Server mit den neuen IPv6-Adressen aktualisiert werden.	„Konfiguration der Namen-Services-Unterstützung für IPv6“ auf Seite 213

Szenario einer IPv6-Netzwerktopologie

Die Aufgaben in diesem Kapitel beschreiben die Planung zur Einführung von IPv6-Services in einem typischen Unternehmensnetzwerk. Die folgende Abbildung zeigt das in diesem Kapitel verwendete Netzwerk. Ihr geplantes IPv6-Netzwerk umfasst möglicherweise alle oder nur einige der Netzwerklinks, die in dieser Abbildung aufgeführt sind.

ABBILDUNG 4–1 Szenario einer IPv6-Netzwerktopologie

Hosts
Hosts
Hosts
LDAP-Server
Mail-Server
DNS-Server
IPv4 192.168.4.0
IPv6 Teilnetz 4
IPv4 192.168.2.0
IPv6 Teilnetz 2
Router 2
Router
Router
Router
Firewall
Netzwerk-Backbone
IPv4 192.168.1.0
IPv6 Teilnetz 1
172.16.85.0
Web-Server
IPv4 192.168.3.0
IPv6 Teilnetz 3
DMZ
NFS-Server
FTP-Server
Router 1
(Grenzrouter)
Firewall
ISP
Internet

Dieses Szenario eines Unternehmensnetzwerks besteht aus fünf Teilnetzen mit vorhandenen IPv4-Adressen. Die Links im Netzwerk tauschen Daten direkt mit den administrativen Teilnetzen aus. Die vier internen Netzwerke werden mit privaten IPv4-Adressen gemäß RFC 1918 gezeigt. Dies ist eine häufig verwendete Lösung bei einem Mangel an IPv4-Adressen. Das Adressierungsschema dieser internen Netzwerke ist:

- Teilnetz 1 ist das interne Netzwerk-Backbone `192.168.1`.
- Teilnetz 2 ist das interne Netzwerk `192.168.2` mit LDAP, `sendmail` und DNS-Servern.
- Teilnetz 3 ist das interne Netzwerk `192.168.3` mit den NFS-Servern des Netzwerks.

- Teilnetz 4 ist das interne Netzwerk `192.168.4`, das bestimmte Hosts für die Angestellten des Unternehmens enthält.

Das externe, öffentliche Netzwerk `172.16.85` fungiert als DMZ des Unternehmens. Dieses Netzwerk enthält Webserver, anonyme FTP-Server und andere Ressourcen, die das Netzwerk zur Verfügung stellt. Router 2 führt eine Firewall aus und trennt das öffentliche Netzwerk `172.16.85` vom internen Backbone. Am anderen Ende der DMZ führt Router 1 eine Firewall aus und dient als Grenzserver des Unternehmensnetzwerks.

Die öffentliche DMZ in Abbildung 4–1 hat die private RFC 1918-Adresse `172.16.85`. In der Realität muss die öffentliche DMZ eine registrierte IPv4-Adresse haben. Die meisten IPv4-Standorte verwenden eine Kombination aus öffentlichen Adressen und privaten RFC 1918-Adressen. Wenn Sie jedoch IPv6 einführen, ändert sich das Konzept der öffentlichen und der privaten Adressen. Da IPv6 über einen größeren Adressraum verfügt, werden die öffentlichen IPv6-Adressen für sowohl private als auch öffentliche Netzwerke verwendet.

Vorbereiten eines bestehenden Netzwerks zur Unterstützung von IPv6

Hinweis – Das Dual-Stack-Protokoll von Oracle Solaris unterstützt gleichzeitig IPv4- und IPv6-Vorgänge. Während und nach dem Deployment von IPv6 in Ihrem Netzwerk können IPv4–bezogene Operationen weiterhin erfolgreich durchgeführt werden.

IPv6 fügt einem bestehenden Netzwerk neue Funktionen hinzu. Aus diesem Grund müssen Sie bei der ersten Einführung von IPv6 sicherstellen, dass Sie keine Vorgänge unterbrechen, die mit IPv4 ausgeführt werden. In den Themen in diesem Abschnitt wird beschrieben, wie Sie IPv6 schrittweise in ein bestehendes Netzwerk integrieren.

Vorbereiten der Netzwerktopologie auf die Unterstützung von IPv6

Der erste Schritt bei der Einführung von IPv6 besteht darin, festzustellen, ob die vorhandenen Entitäten in Ihrem Netzwerk IPv6 unterstützen. In den meisten Fällen kann die Netzwerktopologie – Kabel, Router und Hosts – nach der Einführung von IPv6 unverändert weiterverwendet werden. Eventuell müssen Sie jedoch vorhandene Hardware und Anwendungen für IPv6 vorbereiten, bevor Sie die IPv6-Adressen für die Netzwerkschnittstellen konfigurieren.

Überprüfen Sie, ob die Hardware in Ihrem Netzwerk auf IPv6 aufgerüstet werden kann. Lesen Sie beispielsweise die Dokumentation der Hersteller zur IPv6-Konformität der folgenden Hardwareklassen:

- Router
- Firewalls
- Server
- Switches

Hinweis – Alle Vorgänge in diesem Teil gehen davon aus, dass Ihre Netzwerkausrüstung (insbesondere die Router) auf IPv6 aufgerüstet werden können.

Einige Router-Modelle können nicht auf IPv6 aufgerüstet werden. Weitere Informationen und eine Lösungsmöglichkeit finden Sie unter „IPv4-Router kann nicht auf IPv6 aufgerüstet werden“ auf Seite 249.

Vorbereiten der Netzwerkservices auf die Unterstützung von IPv6

Die folgenden typischen IPv6-Netzwerkservices in der aktuellen Oracle Solaris-Version sind IPv6-konform:

- `sendmail`
- NFS
- HTTP (Apache 2.x oder Orion)
- DNS
- LDAP

Der IMAP-Mailservice kann nur unter IPv4 ausgeführt werden.

Knoten, die für IPv6 konfiguriert wurden, können IPv4-Services ausführen. Wenn Sie IPv6 aktivieren, akzeptieren nicht alle Services IPv6-Verbindungen. Services, die zu IPv6 portiert wurden, akzeptieren eine Verbindung. Services, die nicht zu IPv6 portiert worden, arbeiten mit der IPv4-Hälfte des Protokollstapel weiter.

Nach dem Aufrüsten von Services auf IPv6 können eventuell Probleme auftreten. Ausführliche Informationen finden Sie unter „Probleme beim Aufrüsten von Services auf IPv6“ auf Seite 249.

Vorbereiten von Servern auf die Unterstützung von IPv6

Da Server als IPv6-Hosts betrachtet werden, werden ihre IPv6-Adressen vom Neighbor Discovery-Protokoll automatisch konfiguriert. Viele Server sind jedoch mit mehreren Netzwerkschnittstellenkarten (NICs) ausgestattet, die im Rahmen von Wartungs- oder Reparaturarbeiten ausgetauscht werden können. Wenn Sie eine NIC austauschen, erzeugt das Neighbor Discovery-Protokoll automatisch eine neue Schnittstellen-ID für diese NIC. Dieses Verhalten ist für bestimmte Server nicht akzeptabel.

Aus diesem Grund sollten Sie die Schnittstellen-ID-Komponente der IPv6-Adresse jeder Schnittstelle auf dem Server manuell konfigurieren. Anweisungen finden Sie unter „So konfigurieren Sie ein benutzerdefiniertes IPv6-Token“ auf Seite 200. Wenn Sie später eine vorhandene NIC austauschen müssen, wird die bereits konfigurierte IPv6-Adresse automatisch für die neue NIC übernommen.

▼ So bereiten Sie Netzwerkservices auf die Unterstützung von IPv6 vor

1 Aktualisieren Sie die folgenden Netzwerkservices zur Unterstützung von IPv6:

- Mail-Server
- NIS-Server
- NFS

Hinweis – LDAP unterstützt IPv6, ohne dass IPv6-spezifische Konfigurationsschritte durchgeführt werden müssen.

---

2 Stellen Sie sicher, dass Ihre Firewall-Hardware IPv6-konform ist.

Anweisungen finden Sie in der jeweiligen Firewall-bezogenen Dokumentation.

3 Stellen Sie sicher, dass andere Services in Ihrem Netzwerk auf IPv6 portiert wurden.

Weitere Informationen finden Sie in den Marketingsunterlagen und der jeweiligen Softwaredokumentation.

4 Falls die folgenden Services an Ihren Standorten bereitgestellt werden, stellen Sie sicher, dass Sie die erforderlichen Maßnahmen für diese Services eingeleitet haben:

- Firewalls

  Verstärken Sie die für IPv4 angewendeten Richtlinien, so dass sie IPv6 unterstützen. Weitere Informationen zu den Sicherheitsbetrachtungen finden Sie unter „Sicherheitsbetrachtungen bei der Einführung von IPv6“ auf Seite 97.
- Mail

  Erwägen Sie das Hinzufügen der IPv6-Adresse Ihres Mail-Servers zu den MX-Einträgen für das DNS.
- DNS

  Überlegungen zum DNS finden Sie unter „So bereiten Sie das DNS auf die Unterstützung von IPv6 vor“ auf Seite 96.
- IPQoS

Verwenden Sie die gleichen Diffserv-Richtlinien auf einem Host, die für IPv4 eingesetzt wurde. Weitere Informationen finden Sie unter „Classifier-Modul“ auf Seite 907.

5. **Prüfen Sie alle von einem Knoten angebotenen Netzwerkservices, bevor Sie diesen Knoten zu IPv6 konvertieren.**

▼ So bereiten Sie das DNS auf die Unterstützung von IPv6 vor

Die aktuelle Oracle Solaris-Version unterstützt die DNS-Auflösung sowohl auf der Client- als auch auf der Serverseite. Zur Vorbereitung der DNS-Services auf IPv6 führen Sie die folgenden Schritte aus.

Weitere Informationen zur DNS-Unterstützung für IPv6 finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

1. **Stellen Sie sicher, dass der DNS-Server, der die rekursive Namensauflösung durchführt, einen Dual-Stack ausführt (IPv4 und IPv6) oder ob er nur IPv4 unterstützt.**
2. **Bestücken Sie auf dem DNS-Server die DNS-Datenbank mit den entsprechenden AAAA-Einträgen der IPv6-Datenbank in der Weiterleitungszone.**

Hinweis – Server, die mehrere kritische Services ausführen, erfordern besondere Berücksichtigung. Stellen Sie sicher, dass das Netzwerk ordnungsgemäß arbeitet. Achten Sie darauf, dass alle kritischen Services zu IPv6 portiert wurden. Dann fügen Sie die IPv6-Adresse des Servers zur DNS-Datenbank zu.

---

3. **Fügen Sie die zugehörigen PTR-Datensätze für die AAAA-Einträge in die Reverse-Zone ein.**
4. **Fügen Sie entweder nur IPv4-Daten oder sowohl IPv6- als auch IPv4-Daten in den NS-Datensatz ein, der Zonen beschreibt.**

Planung für Tunnel in der Netzwerktopologie

Die IPv6-Implementierung unterstützt als Übergangslösung zahlreiche Tunnel-Konfigurationen, während Ihr Netzwerk zu einer Mischung aus IPv4 und IPv6 migriert. Mithilfe von Tunneln können isolierte IPv6-Netzwerke miteinander kommunizieren. Da der größte Teil des Internet IPv4 ausführt, müssen IPv6-Pakete von Ihrem Standort das Internet über Tunnel zum IPv6-Zielnetzwerk überbrücken.

Im Folgenden sind einige Szenarios für die Verwendung von Tunneln in der IPv6-Netzwerktopologie aufgeführt:

- Der ISP, von dem Sie IPv6-Services erwerben, ermöglicht es Ihnen, einen Tunnel vom Grenzrouter Ihres Standorts zum ISP-Netzwerk zu erzeugen. Abbildung 4–1 zeigt einen solchen Tunnel. In diesem Fall würden Sie einen manuellen IPv6-über-IPv4-Tunnel ausführen.
- Sie verwalten ein großes verteiltes Netzwerk mit IPv4-Konnektivität. Um verteilte Standorte, die IPv6 verwenden, miteinander zu verbinden, können Sie einen automatischen 6to4-Tunnel vom Grenzrouter jedes Teilnetzes ausführen.
- Manchmal kann ein Router in Ihrer Infrastruktur nicht auf IPv6 aufgerüstet werden. In diesem Fall können Sie einen manuellen Tunnel über den IPv4-Router mit zwei IPv6-Routern als Endpunkte erzeugen.

Anweisungen zur Konfiguration von Tunneln finden Sie unter „Aufgaben bei der Konfiguration von Tunneln zur Unterstützung von IPv6 (Übersicht der Schritte)“ auf Seite 204. Konzeptuelle Informationen zu Tunneln finden Sie unter „IPv6-Tunnel“ auf Seite 308.

Sicherheitsbetrachtungen bei der Einführung von IPv6

Bei der Einführung von IPv6 in einem vorhandenes Netzwerk müssen Sie darauf achten, die Sicherheit des Standorts nicht zu beeinträchtigen. Beachten Sie bei der Umsetzung Ihrer IPv6-Lösung die folgenden Sicherheitsaspekte:

- Für IPv6-Pakete und IPv4-Pakete ist der gleiche Filteraufwand erforderlich.
- IPv6-Pakete durchlaufen eine Firewall häufig durch einen Tunnel. Aus diesem Grund sollten Sie eines der folgenden Szenarios verwenden:
  - Sorgen Sie dafür, dass die Firewall den Inhalt des Tunnels inspiziert.
  - Richten Sie eine IPv6-Firewall mit ähnlichen Regeln am anderen Tunnelendpunkt ein.
- Einige Übergangslösungen verwenden IPv6-über-UDP-über-IPv4-Tunnel. Diese Lösungen sind eventuell gefährlich, da sie die Firewall kurzschließen.
- IPv6-Knoten sind global von Punkten außerhalb des Unternehmensnetzwerks aus erreichbar. Wenn Ihre Sicherheitsrichtlinie öffentlichen Zugriff verbietet, müssen Sie strengere Richtlinien für die Firewall einrichten. Eventuell sollten Sie die Firewall als eine statusbehaftete Firewall konfigurieren.

Dieses Buch beschreibt Sicherheitsmerkmale, die innerhalb einer IPv6-Implementierung verwendet werden können.

- Die IP-Sicherheitsarchitektur (IPsec) ermöglicht Ihnen, einen kryptografischen Schutz für IPv6-Pakete einzurichten. Weitere Informationen hierzu finden Sie in Kapitel 19, „IP Security Architecture (Übersicht)“.

- Der Internet Key Exchange (IKE) ermöglicht Ihnen, öffentliche Schlüsselauthentifizierung für IPv6-Pakete zu verwenden. Weitere Informationen hierzu finden Sie in Kapitel 22, „Internet Key Exchange (Übersicht)".

Vorbereiten eines IPv6-Adressierungsplans

Ein wichtiger Teil beim Übergang von IPv4 zu IPv6 ist die Entwicklung eines Adressierungsplans. Zu dieser Aufgabe gehören die folgenden Vorbereitungsmaßnahmen:

- „Beziehen eines Standortpräfix" auf Seite 98
- „Erstellen eines IPv6-Nummerierungsschemas" auf Seite 98

Beziehen eines Standortpräfix

Bevor Sie IPv6 konfigurieren können, müssen Sie ein Standortpräfix beziehen. Das Standortpräfix dient allen Knoten in Ihrer IPv6-Implementierung zum Ableiten von IPv6-Adressen. Eine Einführung in Standortpräfixe finden Sie unter „Präfixe in IPv6" auf Seite 80.

Jeder ISP, der IPv6 unterstützt, kann Ihrer Organisation ein 48-Bit-IPv6-Standortpräfix bereitstellen. Falls Ihr aktueller ISP nur IPv4 unterstützt, können Sie einen anderen ISP zur Unterstützung von IPv6 verwenden, während Ihr aktueller ISP für die IPv4-Unterstützung sorgt. In diesem Fall können Sie eine von mehreren Problemumgebungen wählen. Weitere Informationen finden Sie unter „Der aktuelle ISP unterstützt IPv6 nicht" auf Seite 249.

Handelt es sich bei Ihrem Unternehmen um einen ISP, beziehen Sie die Standortpräfixe für Ihre Kunden von der jeweiligen Internet Registrierungsstelle. Weitere Informationen finden Sie auf der Website der Internet Assigned Numbers Authority (IANA) (`http://www.iana.org`).

Erstellen eines IPv6-Nummerierungsschemas

Sie können die bereits bestehende IPv4-Topologie als Basis für das IPv6-Nummerierungsschema verwenden, es sei denn, das geplante Netzwerk ist vollständig neu.

Erstellen eine Nummerierungsschemas für Teilnetze

Beginnen Sie Ihr Nummerierungsschema, indem Sie vorhandene IPv4-Teilnetze in entsprechende IPv6-Teilnetze umwandeln. Betrachten Sie als Beispiel die in Abbildung 4–1 gezeigten Teilnetze. Teilnetze 1–4 nutzen die RFC 1918 IPv4 private Adresszuweisung für die ersten 16 Bit ihrer Adressen (neben den Ziffern 1–4), um das Teilnetz zu kennzeichnen. Gehen Sie zur Verdeutlichung davon aus, dass dem Standort das IPv6-Präfix `2001:db8:3c4d/48` zugewiesen wurde.

Die folgende Tabelle zeigt, wie die privaten IPv4-Präfixe zu IPv6-Präfixen zugeordnet wurden.

IPv4-Teilnetzpräfix	Entsprechendes IPv6-Teilnetzpräfix
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

Erstellen eines IPv6-Adressierungsplans für Knoten

Bei den meisten Hosts ist die statusfreie, automatische Konfiguration von IPv6-Adressen für deren Schnittstellen eine angemessene, zeitsparende Strategie. Wenn der Host das Standortpräfix von nächsten Router empfängt, erzeugt das Neighbor Discovery-Protokoll automatisch IPv6-Adressen für jede Schnittstelle auf dem Host.

Server benötigen stabile IPv6-Adressen. Wenn Sie die IPv6-Adressen eines Servers nicht manuell konfigurieren, wird automatisch eine neue IPv6-Adresse konfiguriert, wenn eine NIC-Karte in dem Server ausgetauscht wird. Beachten Sie die folgenden Tipps, wenn Sie Adressen für Server erstellen:

- Vergeben Sie aussagekräftige und stabile Schnittstellen-IDs an den Server. Eine Strategie ist das Verwenden eines sequentiellen Nummerierungsschemas für die Schnittstellen-IDs. Beispielsweise könnte die interne Schnittstelle des LDAP-Servers in Abbildung 4–1 die Adresse `2001:db8:3c4d:2::2` erhalten.
- Alternativ können Sie, wenn Sie Ihr IPv4-Netzwerk nicht regelmäßig neu nummerieren, die vorhandenen IPv4-Adressen der Router und Server für deren Schnittstellen-IDs verwenden. Angenommen, die Schnittstelle des Routers 1 zur DMZ in Abbildung 4–1 besitzt die IPv4-Adresse `123.456.789.111` . Sie können diese IPv4-Adresse in eine hexadezimale Zahl umwandeln und dann als Schnittstellen-ID verwenden. Die neue Schnittstellen-ID lautet dann `::7bc8:156F.`

  Verwenden Sie diesen Ansatz jedoch nur dann, wenn Sie die registrierte IPv4-Adresse selbst besitzen, und nicht, wenn Sie die Adresse von einem ISP bezogen haben. Wenn Sie eine IPv4-Adresse verwenden, die Ihnen von einem ISP zugewiesen wurde, stehen Sie vor einem Problem, wenn Sie den Provider wechseln.

Aufgrund der beschränken Anzahl an IPv4-Adressen sind Netzwerkdesigner in der Vergangenheit dazu übergegangen, globale, registrierte Adressen und private RFC 1918-Adressen zu verwenden. Dieses Konzept von globalen und privaten IPv4-Adressen lässt sich jedoch nicht auf IPv6-Adressen übertragen. Sie können globale Unicast-Adressen, die das Standortpräfix enthalten, auf allen Links in einem Netzwerk verwenden, einschließlich der öffentlichen DMZ.

KAPITEL 5

Konfiguration der TCP/IP-Netzwerkservices und IPv4-Adressierung (Aufgaben)

Die TCP/IP-Netzwerkverwaltung erfolgt in zwei Stufen. Die erste Stufe ist das Zusammenstellen der Hardware. Dann konfigurieren Sie die Daemons, Dateien und Services, die das TCP/IP-Protokoll implementieren.

In diesem Kapitel wird beschrieben, wie Sie TCP/IP in einem Netzwerk konfigurieren, das IPv4-Adressierung und -Services implementiert.

Hinweis – Viele in diesem Kapitel beschriebene Aufgaben gelten sowohl für IPv4- als auch für IPv6-konforme Netzwerke. Wenn sich die Konfiguration bei den beiden Adressierungsformaten unterscheidet, werden die IPv4-Konfigurationsschritte in diesem Kapitel aufgeführt. Den Aufgaben in diesem Kapitel ist dann ein Querverweis zu den entsprechenden IPv6-Aufgaben in Kapitel 7, „Konfigurieren eines IPv6-Netzwerks (Vorgehen)“ hinzugefügt.

Dieses Kapitel enthält die folgenden Informationen:

- „Vor der Konfiguration eines IPv6-Netzwerks (Übersicht der Schritte)“ auf Seite 102
- „Festlegen der Host-Konfigurationsmodi“ auf Seite 103
- „Hinzufügen eines Teilnetzes zu einem Netzwerk (Übersicht der Schritte)“ auf Seite 106
- „Konfiguration der Systeme im lokalen Netzwerk. “ auf Seite 108
- „Netzwerkkonfiguration (Übersicht der Schritte)“ auf Seite 107
- „Paketweiterleitung und Routing bei IPv4-Netzwerken“ auf Seite 119
- „Überwachen undModifizieren der Transportschichtservices“ auf Seite 142
- „Verwalten der Schnittstellen in Solaris 10 3/05“ auf Seite 147

Neuerungen in diesem Kapitel

In Solaris 10 8/07 wurden die folgenden Änderungen vorgenommen:

- Sie können das Routing alternativ zum Befehl `routeadm` auch mithilfe der Service Management Facility (SMF) konfigurieren und verwalten. Anweisungen hierzu entnehmen Sie bitte den Verfahren und Beispielen unter „Paketweiterleitung und Routing bei IPv4-Netzwerken“ auf Seite 119 und der Manpage `routeadm(1M)`.
- Die Datei `/etc/inet/ipnodes` wird nicht mehr benötigt. Verwenden Sie `/etc/inet/ipnodes` nur für frühere Oracle Solaris 10-Versionen, wie es in den jeweiligen Verfahren beschrieben wird.

Vor der Konfiguration eines IPv6-Netzwerks (Übersicht der Schritte)

Bevor Sie mit der Konfiguration von TCP/IP beginnen, führen Sie die in der folgenden Tabelle beschriebenen Aufgaben aus. Die Tabelle enthält Beschreibungen zum Zweck der einzelnen Aufgaben sowie die Abschnitte der aktuellen Dokumentation, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
1. Entwerfen der Netzwerktopologie.	Legen Sie das physikalische Layout des Netzwerks fest.	„Einführung in die Netzwerktopologie“ auf Seite 69 und „Topologie eines autonomen IPv4-Systems“ auf Seite 123
2. Beziehen einer Netzwerknummer von Ihrem ISP oder der Regional Internet Registry (RIR).	Beziehen Sie eine registrierte Netzwerknummer, die es den Systemen an Ihrem Standort ermöglicht, extern zu kommunizieren.	„Erstellen eines IPv4-Adressierungsschemas“ auf Seite 62.
3. Planen des IPv4-Adressierungsschemas für das Netzwerk. Hierzu gehört auch die Teilnetz-Adressierung, sofern erforderlich.	Verwenden Sie die Netzwerknummer als Grundlage für Ihren Adressierungsplan.	„Erstellen eines IPv4-Adressierungsschemas“ auf Seite 62.
4. Zusammenstellen der Netzwerkhardware unter Berücksichtigung der Netzwerktopologie. Sicherstellen, dass die Hardware ordnungsgemäß arbeitet.	Richten Sie die Systeme, Netzwerkmedien, Router, Switches, Hubs und Brücken ein, die Sie für die Netzwerktopologie vorgesehen haben.	Die Hardware-Handbücher und „Einführung in die Netzwerktopologie“ auf Seite 69.

Aufgabe	Beschreibung	Siehe
5. Zuweisen von IPv4-Adressen und Hostnamen zu allen Systemen im Netzwerk.	Weisen Sie die IPv4-Adressen während oder nach der Installation des Betriebssystems Oracle Solaris in den entsprechenden Dateien zu.	„Erstellen eines IPv4-Adressierungsschemas" auf Seite 62 und „So ändern Sie die IPv4-Adresse und andere Netzwerkkonfigurationsparameter" auf Seite 114
6. Ausführen der für die Netzwerkschnittstellen und Router erforderlichen Konfigurationssoftware (sofern anwendbar).	Konfigurieren Sie Router und Multihomed-Hosts.	„Planen der Router für Ihr Netzwerk" auf Seite 69 und „Konfiguration eines IPv4-Routers" auf Seite 126 für Informationen zu Routern.
7. Feststellen, welche Namen- oder Verzeichnisservices Ihr Netzwerk verwendet: NIS, LDAP, DNS oder lokalen Dateien.	Konfigurieren Sie den ausgewählten Namen-Service und/oder Verzeichnisservice.	*System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .
8. Auswählen von Domänennamen für Ihr Netzwerk (sofern anwendbar).	Wählen Sie einen Domänennamen für Ihr Netzwerk und registrieren Sie ihn bei InterNIC.	*System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*

Festlegen der Host-Konfigurationsmodi

Als Netzwerkadministrator konfigurieren Sie TCP/IP für die Ausführung auf Hosts und Routern (sofern anwendbar). Sie können diese Systeme so konfigurieren, dass sie die Konfigurationsinformationen aus Dateien auf dem lokalen System oder aus Dateien beziehen, die sich auf anderen Systemen oder im Netzwerk befinden. Dazu benötigen Sie die folgenden Konfigurationsinformationen:

- Hostname jedes Systems
- IP-Adresse jedes Systems
- Domänenname, zu dem jedes System gehört
- Standard-Router
- Auf jedem Netzwerk des Systems verwendete IPv4-Netzmaske

Ein System, das die TCP/IP-Konfigurationsinformationen aus lokalen Dateien bezieht, arbeitet im *lokale Dateien-Modus*. Ein System, das die TCP/IP-Konfigurationsinformationen von einem Remote-Netzwerkserver bezieht, arbeitet im *Netzwerkclient-Modus*.

Systeme, die im lokale Dateien-Modus ausgeführt werden sollten

Damit ein System im lokale Dateien-Modus ausgeführt werden kann, muss es über lokale Kopien der TCP/IP-Konfigurationsdateien verfügen. Diese Dateien werden unter „TCP/IP-Konfigurationsdateien" auf Seite 253 beschrieben. Das System sollte über eine eigene Festplatte verfügen, obwohl diese Empfehlung nicht strikt eingehalten werden muss.

Die meisten Server sollten im lokale Dateien-Modus ausgeführt werden. Diese Anforderung gilt für die folgenden Server:

- Netzwerkkonfigurationsserver
- NFS-Server
- Namen-Server, die NIS-, LDAP- oder DNS-Services bereitstellen
- Mail-Server

Darüber hinaus sollten Router im lokale Dateien-Modus ausgeführt werden.

Systeme, die ausschließlich als Druckserver fungieren, müssen nicht im lokale Dateien-Modus ausgeführt werden. Ob einzelne Hosts im lokale Dateien-Modus ausgeführt werden sollten, hängt von der Größe Ihres Netzwerks ab.

Wenn Sie ein sehr kleines Netzwerk ausführen, ist der Aufwand zur Verwaltung dieser Dateien auf den einzelnen Hosts vertretbar. Umfasst Ihr Netzwerk jedoch hunderte von Hosts, wird diese Aufgabe zu umfangreich, selbst dann, wenn das Netzwerk in mehrere administrative Teildomänen aufgeteilt ist. Aus diesem Grund ist der lokale Dateien-Modus für große Netzwerke wenig effizient. Da Router und Server jedoch selbstständig sein müssen, sollten sie im lokale Dateien-Modus konfiguriert werden.

Netzwerkkonfigurationsserver

Netzwerkkonfigurationsserver sind Server, die Hosts, die im Netzwerkclient-Modus konfiguriert wurden, TCP/IP-Konfigurationsinformationen bereitstellen. Diese Server unterstützen die folgenden drei Boot-Protokolle:

- RARP – Das Reverse Address Resolution Protocol (RARP) ordnet Ethernet-Adressen (48 Bit) IPv4-Adressen (32 Bit) zu. Dies ist das umgekehrte ARP-Protokoll. Wenn Sie RARP auf einem Netzwerkkonfigurationsserver ausführen, beziehen Hosts, die im Netzwerkclient-Modus ausgeführt werden, ihre IP-Adressen und die TCP/IP-Konfigurationsdateien vom Server. RARP-Services werden vom `in.rarpd`-Daemon ermöglicht. Weitere Informationen finden Sie in der Manpage `in.rarpd`(1M).
- TFTP – Das Trivial File Transfer Protocol (TFTP) ist eine Anwendung, die Dateien zwischen Remote-Systemen überträgt. Der `in.tftpd`-Daemon führt TFTP-Services aus und ermöglicht eine Dateiübertragung zwischen Netzwerkkonfigurationsservern und deren Netzwerkclients. Weitere Informationen finden Sie in der Manpage `in.tftpd`(1M).

- Bootparams – Das Bootparams-Protokoll stellt Parameter für den Boot-Vorgang zur Verfügung, die von allen Clients benötigt werden, die nicht aus dem Netzwerk gebootet werden. Diese Services führt der `rpc.bootparamd`-Daemon aus. Weitere Informationen finden Sie in der Manpage `bootparamd(1M)`.

Netzwerkkonfigurationsserver können auch als NFS-Dateiserver fungieren.

Wenn Sie Hosts als Netzwerkclients konfigurieren, müssen Sie auch mindestens ein System in Ihrem Netzwerk als Netzwerkkonfigurationsserver einrichten. Ist Ihr Netzwerk in Teilnetze aufgeteilt, muss in jedem Teilnetz mit Netzwerkclients mindestens ein Netzwerkkonfigurationsserver vorhanden sein.

Als Netzwerkclients konfigurierte Systeme

Ein Host, der die Konfigurationsinformationen von einem Netzwerkkonfigurationsserver bezieht, arbeitet im Netzwerkclient-Modus. Systeme, die als Netzwerkclients konfiguriert sind, benötigen keine lokalen Kopien der TCP/IP-Konfigurationsdateien.

Der *Netzwerkclient-Modus* vereinfacht die Verwaltung von großen Netzwerken. Der Netzwerkclient-Modus minimiert die Anzahl an Konfigurationsaufgaben, die Sie auf den einzelnen Hosts durchführen müssen. Der Netzwerkclient-Modus stellt sicher, dass alle Systeme im Netzwerk den gleichen Konfigurationsstandard aufweisen.

Der Netzwerkclient-Modus kann auf allen Computertypen konfiguriert werden. Beispielsweise können Sie den Netzwerkclient-Modus auf eigenständigen Systemen konfigurieren.

Gemischte Konfigurationen

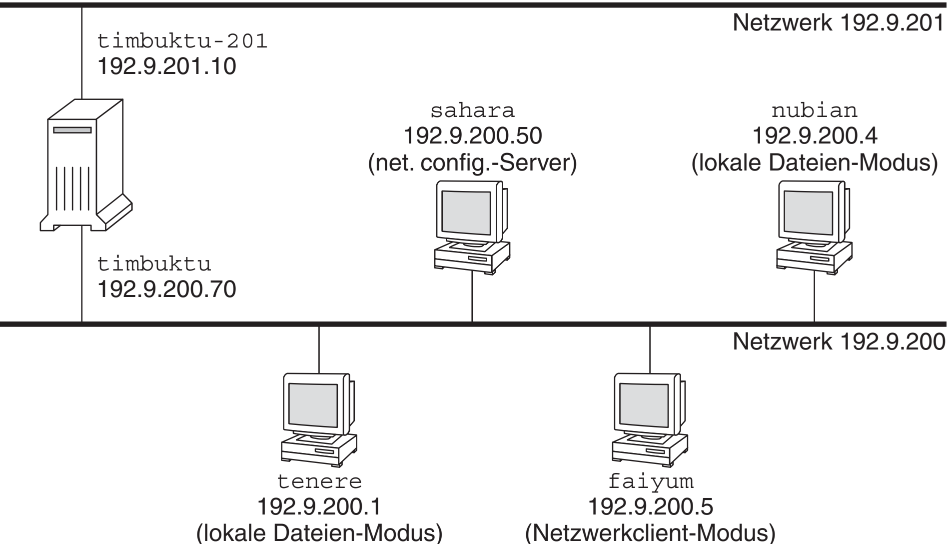
Konfigurationen sind nicht auf entweder den lokale Dateien-Modus oder den Netzwerkclient-Modus beschränkt. Router und Server sollten immer im lokale Dateien-Modus konfiguriert sein. Für Hosts können Sie jedoch eine beliebige Kombination aus lokale Dateien- und Netzwerkclient-Modus wählen.

IPv4-Netzwerktopologie – Szenario

Abbildung 5–1 zeigt die Hosts in einem fiktiven Netzwerk mit der Netzwerknummer `192.9.200`. Das Netzwerk verfügt über einen Netzwerkkonfigurationsserver mit der Bezeichnung `sahara`. Die Hosts `tenere` und `nubian` verfügen über eigene Festplatten und werden im lokale Dateien-Modus ausgeführt. Der Host `faiyum` verfügt ebenfalls über eine Festplatte, dieses System arbeitet aber im Netzwerkclient-Modus.

Das System `timbuktu` ist als Router konfiguriert. Das System verfügt über zwei Netzwerkschnittstellen. Die erste Schnittstelle heißt `timbuktu` und gehört zum Netzwerk `192.9.200`. Die zweite Schnittstelle heißt `timbuktu-201` und gehört zum Netzwerk `192.9.201` . Beide Netzwerke befinden sich in der Organisationsdomäne `deserts.worldwide.com` .

ABBILDUNG 5–1 Hosts in einem IPv4-Netzwerktopologie-Szenario



Hinzufügen eines Teilnetzes zu einem Netzwerk (Übersicht der Schritte)

Um von einem Netzwerk, in dem kein Teilnetz verwendet wird, zu einem Netzwerk zu wechseln, in dem Teilnetze verwendet werden, müssen Sie die in der folgenden Tabelle beschriebenen Aufgaben ausführen.

Hinweis – Die Informationen in diesem Abschnitt gelten nur für IPv4-Teilnetze. Informationen zur Planung von IPv6-Teilnetzen finden Sie unter „Vorbereiten der Netzwerktopologie auf die Unterstützung von IPv6“ auf Seite 93 und „Erstellen eine Nummerierungsschemas für Teilnetze“ auf Seite 98.

In der folgenden Tabelle sind die Aufgaben beschrieben, die zum Hinzufügen eines Teilnetzes zum Netzwerk erforderlich sind. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen Aufgaben sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
1. Feststellen, ob Ihre Netzwerktopologie Teilnetze erfordert.	Legen Sie die neue Teilnetztopologie fest. Bestimmen Sie die Positionen, an denen sich Router und Hosts im Teilnetz befinden sollen.	„Planen der Router für Ihr Netzwerk" auf Seite 69, „Was versteht man unter Subnetting?" auf Seite 260 und „Netzwerkklassen" auf Seite 274
2. Zuweisen der IP-Adressen der neuen Teilnetznummer zu den Systemen, die Mitglieder des Teilnetzes werden.	Konfigurieren Sie die IP-Adressen, die die neue Teilnetznummer verwenden, entweder während der Installation von Oracle Solaris oder später in der `/etc/hostname`*Schnittstelle*-Datei.	„Festlegen eines IP-Adressierungsformats für Ihr Netzwerk" auf Seite 58
3. Konfiguration der Netzmaske des Teilnetzes auf allen künftigen Systemen im Teilnetz.	Bearbeiten Sie die Datei `/etc/inet/netmasks`, wenn Sie die Netzwerkclients manuell konfigurieren. Alternativ stellen Sie dem Oracle Solaris-Installationsprogramm die Netzmaske bereit.	„`netmasks`-Datenbank" auf Seite 260 und „Erstellen der Netzwerkmaske für IPv4-Adressen" auf Seite 261
4. Geben Sie die neuen IP-Adressen aller Systeme im Teilnetz in die Netzwerkdatenbanken ein.	Ändern Sie auf allen Hosts die Datei `/etc/inet/hosts`und (in Solaris 10 11/06 und früheren Releases) die Datei `/etc/inet/ipnodes`, sodass sie die neuen Host-Adressen widerspiegeln.	„`hosts`-Datenbank" auf Seite 255
5. Starten Sie alle Systeme neu.		

Netzwerkkonfiguration (Übersicht der Schritte)

In der folgenden Tabelle werden zusätzliche Aufgaben aufgeführt, die auszuführen sind, nachdem von einer Netzwerkkonfiguration ohne Teilnetze auf ein Netzwerk umgestellt wurde, in dem Teilnetze verwendet werden. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen Aufgaben sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
Konfiguration eines Hosts für den lokale Dateien-Modus.	Bearbeiten Sie die Dateien `nodename`, `hostname`, `hosts`, `defaultdomain`, `defaultrouter` und `netmasks`.	„So konfigurieren Sie einen Host für den lokale Dateien-Modus" auf Seite 109
Einrichten eines Netzwerkkonfigurationsservers.	Aktivieren Sie den `in.tftp`-Daemon und Bearbeiten Sie die Dateien `hosts`, `ethers` und `bootparams`.	„So richten Sie einen Netzwerkkonfigurationsserver ein" auf Seite 112
Konfiguration eines Hosts für den Netzwerkclient-Modus.	Erstellen Sie die Datei `hostname`, Bearbeiten Sie die Datei `hosts` und Löschen Sie die Dateien `nodename` und `defaultdomain`, sofern sie vorhanden sind.	„So konfigurieren Sie Hosts für den Netzwerkclient-Modus" auf Seite 113
Festlegen einer Routing-Strategie für den Netzwerkclient.	Legen Sie fest, ob statisches oder dynamisches Routing auf dem Host verwendet werden soll.	„So aktivieren Sie statisches Routing auf einem Host mit einer Schnittstelle" auf Seite 138 und „So aktivieren Sie das dynamische Routing auf einem Host mit einer Schnittstelle" auf Seite 140.
Bearbeiten der vorhandenen Netzwerkkonfiguration.	Ändern Sie den Hostnamen, die IP-Adresse sowie andere Parameter, die während der Installation eingerichtet oder zu einem späteren Zeitpunkt konfiguriert wurden.	„So ändern Sie die IPv4-Adresse und andere Netzwerkkonfigurationsparameter" auf Seite 114

Konfiguration der Systeme im lokalen Netzwerk.

Die Installation der Netzwerksoftware erfolgt zusammen mit der Installation der Betriebssystemsoftware. Hierbei müssen bestimmte IP-Konfigurationsparameter in den entsprechenden Dateien gespeichert werden, so dass sie beim Booten eingelesen werden können.

Zur Netzwerkkonfiguration gehört auch das Erstellen oder Bearbeiten der Netzwerkkonfigurationsdateien. Wie die Konfigurationsinformationen dann dem Systemkernel bereitgestellt werden, hängt von verschiedenen Dingen ab. Die Verfügbarkeit hängt davon ab, ob diese Dateien lokal gespeichert werden (lokale Dateien-Modus), oder ob sie vom Netzwerkkonfigurationsserver abgerufen werden (Netzwerkclient-Modus).

Bei der Netzwerkkonfiguration werden die folgenden Parameter angegeben:

- Die IP-Adresse jeder Netzwerkschnittstelle in jedem System.

- Der Host-Name jedes Systems im Netzwerk. Sie können den Host-Namen in eine lokale Datei oder in eine Namen-Service-Datenbank eingeben.
- Den NIS-, LDAP- oder DNS-Domänennamen, indem sich das System befindet (sofern anwendbar).
- Die standardmäßigen Router-Adressen. Diese Informationen geben Sie an, wenn eine einfache Netzwerktopologie nur über einen Router verfügt, der an jedes Netzwerk angehängt ist. Sie geben diese Informationen auch dann an, wenn Ihre Router kein Routing-Protokoll wie das Router Discovery Server Protocol (RDISC) oder das Router Information Protocol (RIP) ausführen. Weitere Informationen zu Standard-Routern finden Sie unter „Paketweiterleitung und Routing bei IPv4-Netzwerken" auf Seite 119. Eine Liste der von Oracle Solaris unterstützten Routing-Protokolle finden Sie in Tabelle 5–1
- Teilnetzmaske (nur erforderlich für Netzwerke mit Teilnetzen).

Wenn das Oracle Solaris-Installationsprogramm mehrere Schnittstellen auf einem System erkennt, können Sie die zusätzlichen Schnittstellen optional während der Installation konfigurieren. Vollständige Anweisungen hierzu finden Sie im *Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen*.

Diese Kapitel enthalten Informationen zum Erstellen und Bearbeiten von lokalen Konfigurationsdateien. Informationen zum Arbeiten mit Namen-Service-Datenbanken finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

▼ So konfigurieren Sie einen Host für den lokale Dateien-Modus

Mit dem folgenden Verfahren konfigurieren Sie TCP/IP auf einem Host, der im lokale Dateien-Modus ausgeführt wird.

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Wechseln Sie in das Verzeichnis** `/etc`**.**

3. **Überprüfen Sie, ob der korrekte Hostname in der Datei** `/etc/nodename` **ausgewählt ist.**

   Wenn Sie den Hostnamen eines Systems während der Installation von Oracle Solaris angegeben haben, wurde dieser Hostname bereits in die Datei `/etc/nodename` eingetragen. Achten Sie darauf, dass der Eintrag für den Knotennamen den richtigen Hostnamen für das System enthält.

4 Überprüfen Sie, ob für jede Netzwerkschnittstelle im System eine `/etc/hostname.`*interface*-Datei vorhanden ist.

Informationen zur Dateisyntax und grundlegende Informationen zur Datei `/etc/hostname.`*Schnittstelle* finden Sie unter „Grundlagen zur Verwaltung physikalischer Schnittstellen“ auf Seite 165.

Das Oracle Solaris-Installationsprogramm verlangt, dass während der Installation mindestens eine Schnittstelle konfiguriert wird. Die erste von Ihnen konfigurierte Schnittstelle wird automatisch zur *primären Netzwerkschnittstelle*. Das Installationsprogramm erstellt eine `/etc/hostname.`*Schnittstelle*-Datei für die primäre Schnittstelle sowie für alle weiteren Schnittstellen, die Sie optional während der Installation konfigurieren.

Wenn Sie zusätzliche Schnittstellen während der Installation konfigurieren, prüfen Sie, ob jede über eine entsprechende `/etc/hostname.`*Schnittstelle*-Datei verfügt. Während der Installation von Oracle Solaris müssen Sie keine zusätzlichen Schnittstellen konfigurieren. Wenn Sie jedoch zu einem späteren Zeitpunkt Schnittstellen zum System hinzufügen, müssen diese manuell konfiguriert werden.

Anweisungen zur manuellen Konfiguration von Schnittstellen finden Sie unter „Verwalten der Schnittstellen in Solaris 10 3/05“ auf Seite 147 bzw. „So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation“ auf Seite 159 für Releases ab Solaris 10 1/06.

5 Stellen Sie bei Solaris 10 11/06 und früheren Releases sicher, dass die Einträge in der `/etc/inet/ipnodes`-Datei noch aktuell sind.

Die `/etc/inet/ipnodes`-Datei wird vom Oracle Solaris 10-Installationsprogramm erstellt. Diese Datei enthält den Knotennamen und die IPv4-Adresse (sowie die IPv6-Adresse, sofern vorhanden) jeder Schnittstelle, die während der Installation konfiguriert wurde.

Für Einträge in der `/etc/inet/ipnodes`-Datei verwenden Sie das folgende Format:

IP-address node-name nicknames...

Nicknamen sind zusätzliche Namen, unter denen eine Schnittstelle bekannt ist.

6 Prüfen Sie, ob die Einträge in der `/etc/inet/hosts`-Dateien noch aktuell sind.

Das Oracle Solaris-Installationsprogramm erstellt Einträge für die primäre Netzwerkschnittstelle, die Loopback-Adresse und, sofern anwendbar, für alle weiteren Schnittstellen, die während der Installation konfiguriert wurden.

a. **Achten Sie darauf, dass die in der `/etc/inet/hosts`-Datei vorhandenen Einträge noch aktuell sind.**

b. **(Optional) Fügen Sie die IP-Adressen und die entsprechenden Namen aller Netzwerkschnittstellen hinzu, die dem lokalen Host nach der Installation hinzugefügt wurden.**

c. **(Optional) Fügen Sie die IP-Adresse bzw. -adressen des Dateiservers hinzu, wenn das** `/usr`**-Dateisystem NFS-gemountet ist.**

7 **Geben Sie den vollständig qualifizierten Domänennamen des Hosts in die** `/etc/defaultdomain`**-Datei ein.**

Angenommen, der Host `tenere` ist Teil der Domäne `deserts.worldwide.com`. In diesem Fall würden Sie `deserts.worldwide.com` in die `/etc/defaultdomain`-Datei eingeben. Weitere Informationen finden Sie unter „`/etc/defaultdomain`-Datei" auf Seite 255.

8 **Geben Sie den Routernamen in die** `/etc/defaultrouter`**-Datei ein.**

Informationen zu dieser Datei finden Sie unter „`/etc/defaultrouter`-Datei" auf Seite 255.

9 **Geben Sie den Namen des Standard-Routers und dessen IP-Adressen in die** `/etc/inet/hosts`**-Datei ein.**

Wie unter „So konfigurieren Sie Hosts für den Netzwerkclient-Modus" auf Seite 113 beschrieben, stehen weitere Routing-Optionen zur Verfügung. Sie können die Optionen bei der Konfiguration eines lokale Dateien-Modus anwenden.

10 **Fügen Sie eine Netzwerkmaske für Ihr Netzwerk hinzu (sofern anwendbar):**

- Wenn der Host seine IP-Adresse von einem DHCP-Server bezieht, müssen Sie die Netzwerkmaske nicht angeben.
- Wenn Sie im Netzwerk dieses Clients einen NIS-Server eingerichtet haben, können Sie die `netmask`-Informationen in die entsprechende Datenbank auf dem Server eingeben.
- Bei allen anderen Bedingungen führen Sie folgende Schritte aus:

a. **Geben Sie die Netzwerknummer und die Netzmaske in die** `/etc/inet/netmasks`**-Datei ein.**

Verwenden Sie die folgende Syntax:

```
network-number netmask
```

Für die Klasse C-Netzwerknummer `192.168.83` geben Sie z. B. Folgendes ein:

```
192.168.83.0    255.255.255.0
```

Bei CIDR-Adressen wandeln Sie das Netzwerkpräfix in die entsprechende getrennte dezimale Notation um. Netzwerkpräfixe und deren Entsprechungen in der getrennten dezimalen Notation finden Sie in Tabelle 2–3. Für das CIDR-Netzwerkpräfix `192.168.3.0/22` geben Sie z. B. Folgendes ein.

```
192.168.3.0 255.255.252.0
```

b. **Ändern Sie die Suchreihenfolge für Netzmasken in der** `/etc/nsswitch.conf`**-Datei, so dass lokale Dateien zuerst durchsucht werden:**

```
netmasks:   files nis
```

11 Starten Sie das System neu.

▼ So richten Sie einen Netzwerkkonfigurationsserver ein

Informationen zum Einrichten von Installations- und Boot-Servern finden Sie in *Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen*

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Wechseln Sie in das Root-Verzeichnis (`/`) des künftigen Netzwerkkonfigurationsservers.

3 Schalten Sie den `in.tftpd`-Daemon ein, indem Sie das Verzeichnis `/tftpboot` erstellen:

```
# mkdir /tftpboot
```

Mit diesem Befehl wird das System als ein TFTP-, bootparams- und RARP-Server konfiguriert.

4 Erstellen Sie einen symbolischen Link zum Verzeichnis.

```
# ln -s /tftpboot/. /tftpboot/tftpboot
```

5 Aktivieren Sie die Zeile `tftp` in der `/etc/inetd.conf`-Datei.

Prüfen Sie, ob der Eintrag wie folgt lautet:

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

Diese Zeile verhindert, dass der `in.tftpd`-Daemon andere Dateien außer denen abruft, die sich im `/tftpboot`-Verzeichnis befinden.

6 Nehmen Sie Änderungen an der `hosts`-Datenbank vor.

Fügen Sie die Hostnamen und IP-Adressen jedes Client im Netzwerk hinzu.

7 Nehmen Sie Änderungen an der `ethers`-Datenbank vor.

Erstellen Sie Einträge für jeden Host im Netzwerk, der im Netzwerkclient-Modus ausgeführt wird.

8 Nehmen Sie Änderungen an der `bootparams`-Datenbank vor.

Lesen Sie „`bootparams`-Datenbank“ auf Seite 269. Verwenden Sie einen Platzhalter oder erstellen Sie einen Eintrag für jeden Host, der im Netzwerkclient-Modus ausgeführt wird.

9. **Wandeln Sie den `/etc/inetd.conf`-Eintrag in ein Service Management Facility (SMF)-Servicemanifest um, und aktivieren Sie den resultierenden Service:**

```
# /usr/sbin/inetconv
```

10. **Prüfen Sie, ob der `in.tftpd`-Daemon korrekt arbeitet.**

```
# svcs network/tftp/udp6
```

Es sollte eine Ausgabe ähnlich der Folgenden angezeigt werden:

```
STATE          STIME    FMRI
online         18:22:21 svc:/network/tftp/udp6:default
```

Weitere Informationen:

Verwalten des `in.tftpd`-Daemon

Der `in.tftpd`-Daemon wird von der Service Management Facility verwaltet. Administrative Aktionen am `in.tftpd`-Daemon, z. B. Aktivieren, Deaktivieren oder Neustarten, können mithilfe des Befehls `svcadm` ausgeführt werden. Die Verantwortung für das Initiieren und Neustarten dieses Services wurde an `inetd` delegiert. Mit dem Befehl `inetadm` können Sie Konfigurationsänderungen vornehmen und die Konfigurationsinformationen für den `in.tftpd`-Daemon anzeigen. Der Status des Services kann mithilfe des Befehls `svcs` abgefragt werden. Eine Übersicht zur Service Management Facility finden Sie in Kapitel 18, „Managing Services (Overview)" in *System Administration Guide: Basic Administration*.

Konfiguration der Netzwerkclients

Netzwerkclients beziehen ihre Konfigurationsinformationen von Netzwerkkonfigurationsservern. Daher müssen Sie vor dem Konfigurieren eines Hosts als Netzwerkclient sicherstellen, dass mindestens ein Netzwerkkonfigurationsserver für das Netzwerk eingerichtet ist.

▼ So konfigurieren Sie Hosts für den Netzwerkclient-Modus

Führen Sie die folgenden Schritte auf jedem Host aus, der im Netzwerkclient-Modus konfiguriert werden soll.

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 **Suchen Sie das** `/etc`**-Verzeichnis der** `nodename`**-Datei.**

Wenn eine solche Datei vorhanden ist, löschen Sie sie.

Durch Löschen der `/etc/nodename`-Datei wird das System gezwungen, das Programm `hostconfig` zu verwenden, um Hostnamen, Domänennamen und Router-Adressen vom Netzwerkkonfigurationsserver zu beziehen. Lesen Sie dazu „Konfiguration der Systeme im lokalen Netzwerk. " auf Seite 108.

3 **Erstellen Sie eine** `/etc/hostname.`*Schnittstelle***-Datei, sofern keine vorhanden ist.**

Stellen Sie sicher, dass die Datei leer ist. Eine leere `/etc/hostname.`*Schnittstelle*-Datei sorgt dafür, dass das System die IPv4-Adresse vom Netzwerkkonfigurationsserver bezieht.

4 **Stellen Sie sicher, dass die** `/etc/inet/hosts`**-Datei nur den** `localhost`**-Namen und die IP-Adresse der Loopback-Netzwerkschnittstelle enthält.**

```
# cat /etc/inet/hosts
# Internet host table
#
127.0.0.1       localhost
```

Die IPv4-Loopback-Schnittstelle hat die IP-Adresse `127.0.0.1`

Weitere Informationen finden Sie unter „Loopback-Adresse" auf Seite 257. Die Datei darf die IP-Adresse und den Hostnamen des lokalen Hosts (primärer Netzwerkschnittstelle) nicht enthalten.

5 **Prüfen Sie, ob eine** `/etc/defaultdomain`**-Datei vorhanden ist.**

Wenn eine solche Datei vorhanden ist, löschen Sie sie.

Das `hostconfig`-Programm richtet den Domänennamen automatisch ein. Um den von `hostconfig` eingerichteten Domänennamen zu überschreiben, geben Sie den zu verwendenden Domänennamen in die `/etc/defaultdomain`-Datei ein.

6 **Stellen Sie sicher, dass die Suchpfade in der** `/etc/nsswitch.conf`**-Datei auf dem Client die Namensdienst-Anforderungen für Ihr Netzwerk erfüllt.**

▼ So ändern Sie die IPv4-Adresse und andere Netzwerkkonfigurationsparameter

In diesem Verfahren wird beschrieben, wie Sie IPv4-Adresse, Hostname und andere Netzwerkparameter bei einem bereits installierten System ändern. Mit diesem Verfahren ändern Sie die IP-Adresse eines Servers oder eines mit einem Netzwerk verbundenen eigenständigen Systems. Dieses Verfahren gilt nicht für Netzwerkclients oder -geräte. Die im Folgenden aufgeführten Schritte erstellen eine Konfiguration, die auch nach einem Neustart gültig bleibt.

Hinweis – Die Anweisungen gelten speziell für das Ändern der IPv4-Adresse der primären Netzwerkschnittstelle. Informationen zum Hinzufügen einer weiteren Schnittstelle zum System finden Sie unter „So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation“ auf Seite 159.

Die im Folgenden aufgeführten Schritte verwenden fast ausschließlich die traditionelle getrennte dezimale IPv4-Notation zur Angabe der IPv4-Adresse und der Teilnetzmaske. Alternativ können Sie die CIDR-Notation verwenden, um die IPv4-Adresse in allen anwendbaren Dateien dieses Verfahrens anzugeben. Eine Einführung in die CIDR-Notation finden Sie unter „IPv4-Adressen im CIDR-Format“ auf Seite 59.

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Bei Solaris 10 11/06 und früheren Releases ändern Sie die IP-Adresse nur in der** `/etc/inet/ipnodes`**-Datei oder der entsprechenden** `ipnodes`**-Datenbank.**

   Verwenden Sie die folgende Syntax für jede IP-Adresse, die Sie dem System hinzufügen:

   IP-address host-name, nicknames
   IP-address interface-name, nicknames

   Der erste Eintrag muss die IP-Adresse der primären Netzwerkschnittstelle und der Hostname des Systems sein. Optional können Sie Nicknamen für den Hostnamen angeben. Wenn Sie weitere physikalische Schnittstellen zu einem System hinzufügen, erstellen Sie Einträge in der `/etc/inet/ipnodes`-Datei für die IP-Adressen und weisen diesen Schnittstellen Namen zu.

3. **Ändert sich der Hostname eines Systems, bearbeiten Sie den entsprechenden Eintrag in der** `/etc/nodename`**-Datei.**

4. **Ändern Sie die IP-Adresse und, sofern anwendbar, den Hostnamen in der** `/etc/inet/hosts`**-Datei oder der entsprechenden** `hosts`**-Datenbank.**

5. **Ändern Sie die IP-Adresse in der** `/etc/hostname.`*Schnittstelle***-Datei für die primäre Netzwerkschnittstelle.**

   Sie können eine der folgenden Angaben als Eintrag für die primäre Netzwerkschnittstelle in der `/etc/hostname.`*Schnittstelle*-Datei verwenden:

   - IPv4-Adresse im traditionellen getrennten dezimalen Format

     Verwenden Sie die folgende Syntax:

     IPv4 address subnet mask

Der Eintrag für die Netzmaske ist optional. Wenn Sie die Netzmaske nicht angeben, wird die Standard-Netzmaske übernommen.

Beispiel:

```
# vi hostname.eri0
10.0.2.5 netmask 255.0.0.0
```

- IPv4-Adresse, in der CIDR-Notation, sofern für Ihre Netzwerkkonfiguration anwendbar.

  IPv4 address/network prefix

  Beispiel:

  ```
  # vi hostname.eri0
  10.0.2.5/8
  ```

  Das CIDR-Präfix weist die geeignete Netzmaske für die IPv4-Adresse zu. Beispielsweise gibt die `/8` oben die Netzmaske `255.0.0.0` an.

- Hostname.

  Um den Hostnamen des Systems in der `/etc/hostname.`*Schnittstelle*-Datei zu verwenden, achten Sie darauf, dass der Hostname und die zugehörige IPv4-Adresse auch in der `hosts`-Datenbank angegeben sind.

6 Wenn die Teilnetzmaske geändert wurde, müssen Sie die Teilnetz-Einträge in den folgenden Dateien bearbeiten:

- `/etc/netmasks`
- (Optional) `/etc/hostname.`*Schnittstelle*

7 Hat sich die Teilnetzadresse geändert, müssen Sie die IP-Adresse des Standard-Routers in der `/etc/defaultrouter`**-Datei zur Adresse des neuen Standard-Routers des Teilnetzes ändern.**

8 Starten Sie das System neu.

```
# reboot -- -r
```

Beispiel 5–1 Ändern der IPv4-Adresse und anderer Netzwerkparameter, so dass sie nach einem Neustart gültig bleiben

In diesem Beispiel wird gezeigt, wie die folgenden Netzwerkparameter eines Systems geändert werden, dass in ein anderes Teilnetz verschoben wird:

- Die IP-Adresse der primäre Netzwerkschnittstelle `eri0` wird von `10.0.0.14` zu `192.168.55.14` geändert.
- Der Hostname ändert sich von `myhost` zu `mynewhostname`.
- Die Netzmaske ändert sich von `255.0.0.0` zu `255.255.255.0`.
- Die Adresse des Standard-Routers ändert sich zu `192.168.55.200` .

Prüfen Sie den aktuellen Status des Systems:

```
# hostname
myhost
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.14 netmask ff000000 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
```

Als Nächstes ändern Sie den Hostnamen und die IP-Adresse des Systems `eri0` in den entsprechenden Dateien:

```
# vi /etc/nodename
mynewhostname

In Solaris 10 11/06 and earlier Solaris 10 releases only, do the following:
# vi /etc/inet/ipnodes
192.168.55.14   mynewhostname      #moved system to 192.168.55 net

# vi /etc/inet/hosts
#
# Internet host table
#
127.0.0.1       localhost
192.168.55.14   mynewhostname        loghost
# vi /etc/hostname.eri0
192.168.55.14   netmask  255.255.255.0
```

Schließlich ändern Sie die Netzmaske und die IP-Adresse des Standard-Routers.

```
# vi /etc/netmasks.
.
.
192.168.55.0    255.255.255.0
# vi /etc/defaultrouter
192.168.55.200        #moved system to 192.168.55 net
#
```

Nachdem Sie alle Änderungen vorgenommen haben, booten Sie das System neu.

```
# reboot -- -r
```

Überprüfen Sie, ob die gerade eingerichtete Konfiguration auch nach einem Neustart bestehen bleibt:

```
# hostname
mynewhostname
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.55.14 netmask ffffff00 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
```

Beispiel 5–2 Ändern der IP-Adresse und des Hostnamens nur für die aktuelle Sitzung

In diesem Beispiel wird gezeigt, wie Sie den Hostnamen und die IP-Adresse der primären Netzwerkschnittstelle und die Teilnetzmaske nur für die aktuelle Sitzung ändern. Wenn Sie das System neu starten, nimmt das System wieder die vorherige IP-Adresse und Teilnetzmaske an. Die IP-Adresse der primären Netzwerkschnittstelle `eri0` wird von `10.0.0.14` zu `192.168.34.100` geändert.

```
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.14 netmask ff000000 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
# ifconfig eri0 192.168.34.100 netmask 255.255.255.0 broadcast + up
# vi /etc/nodename
mynewhostname

# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.34.100 netmask ffffff00 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
# hostname
mynewhostname
```

Beispiel 5–3 Ändern der IPv4-Adresse für die aktuelle Sitzung mithilfe der CIDR-Notation

In diesem Beispiel wird gezeigt, wie Sie den Hostnamen und die IP-Adresse mithilfe der CIDR-Notation nur für die aktuelle Sitzung ändern. Wenn Sie das System neu starten, nimmt das System wieder die vorherige IP-Adresse und Teilnetzmaske an. Die IP-Adresse der primären Netzwerkschnittstelle `eri0` wird von `10.0.0.14` zu `192.168.6.25/27` geändert.

```
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.14 netmask ff000000 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
# ifconfig eri0 192.168.6.25/27 broadcast + up
# vi /etc/nodename
mynewhostname
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.06.25 netmask ffffffe0 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
# hostname
mynewhostname
```

Wenn Sie die CIDR-Notation für die IPv4-Adressen verwenden, müssen Sie die Netzmaske nicht angeben. `ifconfig` verwendet die Bezeichnung des Netzwerkpräfix, um die Netzmaske festzulegen. Für das Netzwerk `192.168.6.0/27` legt `ifconfig` die Netzmaske `ffffffe0` fest. Wenn Sie die gebräuchlichere `/24`-Präfixbezeichnung verwenden, wäre die resultierende Netzmaske `ffffff00`. Bei der Konfiguration einer neuen IP-Adresse entspricht das Verwenden der `/24`-Präfixbezeichnung der Angabe der Netzmaske `255.255.255.0` gegenüber `ifconfig`.

Siehe auch Wie Sie die IP-Adresse einer anderen Schnittstelle als der primäre Netzwerkschnittstelle ändern, lesen Sie im *System Administration Guide: Basic Administration* und unter „So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation“ auf Seite 159.

Paketweiterleitung und Routing bei IPv4-Netzwerken

Dieser Abschnitt enthält Verfahren und Beispiele, mit denen gezeigt wird, wie Weiterleitung und Routing für Router und Hosts in IPv4-Netzwerken konfiguriert werden.

Paketweiterleitung ist ein allgemeines Verfahren zum gemeinsamen Nutzen von Informationen auf mehreren Systemen in einem Netzwerk. Pakete werden zwischen einer Ursprungsschnittstelle und einer Zielschnittstelle übertragen, die sich in der Regel in zwei verschiedenen Systemen befinden. Wenn Sie einen Befehl ausgeben oder eine Nachricht an eine nicht-lokale Schnittstelle senden, sendet Ihr System diese Pakete an das lokale Netzwerk. Die Schnittstelle mit der im Paket-Header angegebenen IP-Zieladresse empfängt die Pakete dann vom lokalen Netzwerk. Befindet sich die Zieladresse nicht im lokalen Netzwerk, werden die Pakete an das nächste benachbarte Netzwerk bzw. an den nächsten *Hop* weitergeleitet. Standardmäßig wird die Paketweiterleitung bei der Installation von Oracle Solaris automatisch konfiguriert.

Routing ist der Prozess, bei dem Systeme entscheiden, wohin ein Paket gesendet wird. Routing-Protokolle auf einem System „erkennen“ andere Systeme im lokalen Netzwerk. Befinden sich Ursprungs- und Zielsystem im gleichen lokalen Netzwerk, wird der Pfad eines Paketes zwischen diesen Systemen als *direkte Route* bezeichnet. Muss ein Paket mindestens einen Hop über das Quellsystem hinaus durchlaufen, wird der Pfad zwischen Ursprungs- und Zielsystem als *indirekte Route* bezeichnet. Die Routing-Protokolle lernen den Pfad zu einer Zielschnittstelle und speichern Daten über bekannte Routen in der so genannten *Routing-Tabelle*.

Router sind speziell konfigurierte Systeme mit mehreren physikalischen Schnittstellen, die die Verbindung zu mehreren lokalen Netzwerken herstellen. Aus diesem Grund kann der Router Pakete über das eigene LAN hinaus weiterleiten, unabhängig davon, ob der Router ein Routing-Protokoll ausführt. Weitere Informationen, wie Router Pakete weiterleiten, finden Sie unter „Planen der Router für Ihr Netzwerk“ auf Seite 69.

Routing-Protokolle verarbeiten die Routing-Aktivität eines Systems und pflegen die Angaben über bekannte Routen zu Remote Netzwerken, indem sie Routing-Informationen mit anderen Hosts austauschen. Sowohl Router als auch Hosts können Routing-Protokolle ausführen. Die

Routing-Protokolle auf dem Host kommunizieren mit Routing-Daemons auf anderen Routern und Hosts. Diese Protokolle helfen dem Host zu ermitteln, wohin Pakete weitergeleitet werden. Wenn Netzwerkschnittstellen aktiviert sind, kommuniziert das System automatisch mit den Routing-Daemons. Diese Daemons überwachen die Router in einem Netzwerk und melden die Router-Adressen an die Hosts im lokalen Netzwerk. Einige Routing-Protokolle (aber nicht alle) pflegen sogar Statistiken, die Sie zum Messen der Routing-Leistung verwenden können. Im Gegensatz zur Paketweiterleitung muss das Routing auf einem Oracle Solaris-System explizit konfiguriert werden.

Dieser Abschnitt enthält Aufgaben zur Verwaltung von Paketweiterleitung und Routing auf IPv4-Routern und Hosts. Weitere Informationen zum Routing in IPv6-konformen Netzwerken finden Sie unter „Konfiguration eines IPv6-Routers“ auf Seite 191.

Von Oracle Solaris unterstützte Routing-Protokolle;

Routing Protokolle werden als Interior Gateway Protocols (IGPs), Exterior Gateway Protocols (EGPs) oder als eine Kombination aus beidem klassifiziert. *Interior Gateway Protocols* tauschen Routing-Informationen zwischen Routern in Netzwerken unter gemeinsamer administrativer Kontrolle aus. Bei der in Abbildung 5–3 gezeigten Netzwerktopologie führen die Router ein IGP aus, um Routing-Informationen untereinander auszutauschen. *Exterior Gateway Protocols* ermöglichen es einem Router, der ein lokales Netzwerk mit dem externen Netzwerk verbindet, Informationen mit anderen Routern im externen Netzwerk auszutauschen. Beispielsweise führt ein Router, der ein Unternehmensnetzwerk mit einem ISP verbindet, ein EGP aus, um Routing-Informationen mit seinem Router-Gegenstück beim ISP auszutauschen. Border Gateway Protocol (BGP) ist ein beliebtes EGP, das für die Übertragung von Routing-Informationen zwischen unterschiedlichen Organisationen und IGPs verwendet wird.

Die folgende Tabelle enthält Informationen zu den Oracle Solaris-Routing-Protokollen und verweist auf die entsprechende Dokumentation.

TABELLE 5–1 Oracle Solaris Routing-Protokolle

Protokoll	Zugehöriger Daemon	Beschreibung	Siehe
Routing Information Protocol (RIP)	`in.routed`	IGP, das IPv6-Pakete und eine Routing-Tabelle verwaltet	„So konfigurieren Sie einen IPv4-Router“ auf Seite 126
Internet Control Message Protocol (ICMP) Router Discovery	`in.routed`	Wird von Hosts zum Erfassen eines Routers im Netzwerk verwendet	„So aktivieren Sie statisches Routing auf einem Host mit einer Schnittstelle“ auf Seite 138 und „So aktivieren Sie das dynamische Routing auf einem Host mit einer Schnittstelle“ auf Seite 140
Routing Information Protocol, next generation (RIPng)-Protokoll	`in.ripngd`	IGP, dass IPv6-Pakete und eine Routing-Tabelle verwaltet	„So konfigurieren Sie einen IPv6-konformen Router“ auf Seite 192

TABELLE 5–1 Oracle Solaris Routing-Protokolle *(Fortsetzung)*

Protokoll	Zugehöriger Daemon	Beschreibung	Siehe
Neighbor Discovery (ND)-Protokoll	`in.ndpd`	Gibt das Vorhandensein eines IPv6-Routers bekannt und erkennt das Vorhandensein von IPv6-Hosts in einem Netzwerk	„Konfiguration einer IPv6-Schnittstelle" auf Seite 185

Weiterhin unterstützt Oracle Solaris 10 die Open Source Quagga Routing-Protokoll-Familie. Diese Protokolle befinden sich auf der SFW-Konsolidierungs-CD, obwohl sie nicht zur Oracle Solaris-Distribution gehören. Die folgende Tabelle enthält eine Liste der Quagga-Protokolle:

TABELLE 5–2 OpenSolaris Quagga-Protokolle

Protokoll	Daemon	Beschreibung
RIP-Protokoll	`ripd`	IPv4-Distance Vectoring-IGP, das IPv6-Pakete routet und die Routing-Tabellen an Nachbarn weitergibt.
RIPng	`ripngd`	IPv6 Distance Vectoring-IGP. Routet IPv6-Pakete und pflegt eine Routing-Tabelle.
Open Shortest Path First (OSPF)-Protokoll	`ospfd`	IPv4 Link State-IGP zum Paket-Routing und für High Availability-Netzwerke
Border Gateway Protocol (BGP)	`bgpd`	IPv4- und IPv6-EGP für das Routing über administrative Domänen.

Die folgende Abbildung zeigt ein autonomes System, in dem die Quagga-Routing-Protokolle verwendet werden:

ABBILDUNG 5–2 Unternehmensnetzwerk, in dem Quagga-Protokolle ausgeführt werden

Die Abbildung zeigt ein Unternehmensnetzwerk mit einem autonomen System, das in zwei Routing-Domänen, A und B, aufgeteilt ist. Eine *Routing-Domäne* ist ein Internetzwerk mit einer kohäsiven Routing-Richtlinie – entweder aus administrativen Gründen oder weil die Domäne ein einzelnes Routing-Protokoll ausführt. Beide Domänen in der Abbildung führen Routing-Protokolle aus der Quagga-Protokollfamilie aus.

Routing-Domäne A ist eine OSPF-Domäne, die unter einer einzelnen OSPF-Domänen-ID verwaltet wird. Alle Systeme innerhalb dieser Domäne führen OSPF als Interior Gateway Protocol aus. Zusätzlich zu den internen Hosts und Routern umfasst Domäne A zwei Grenzrouter.

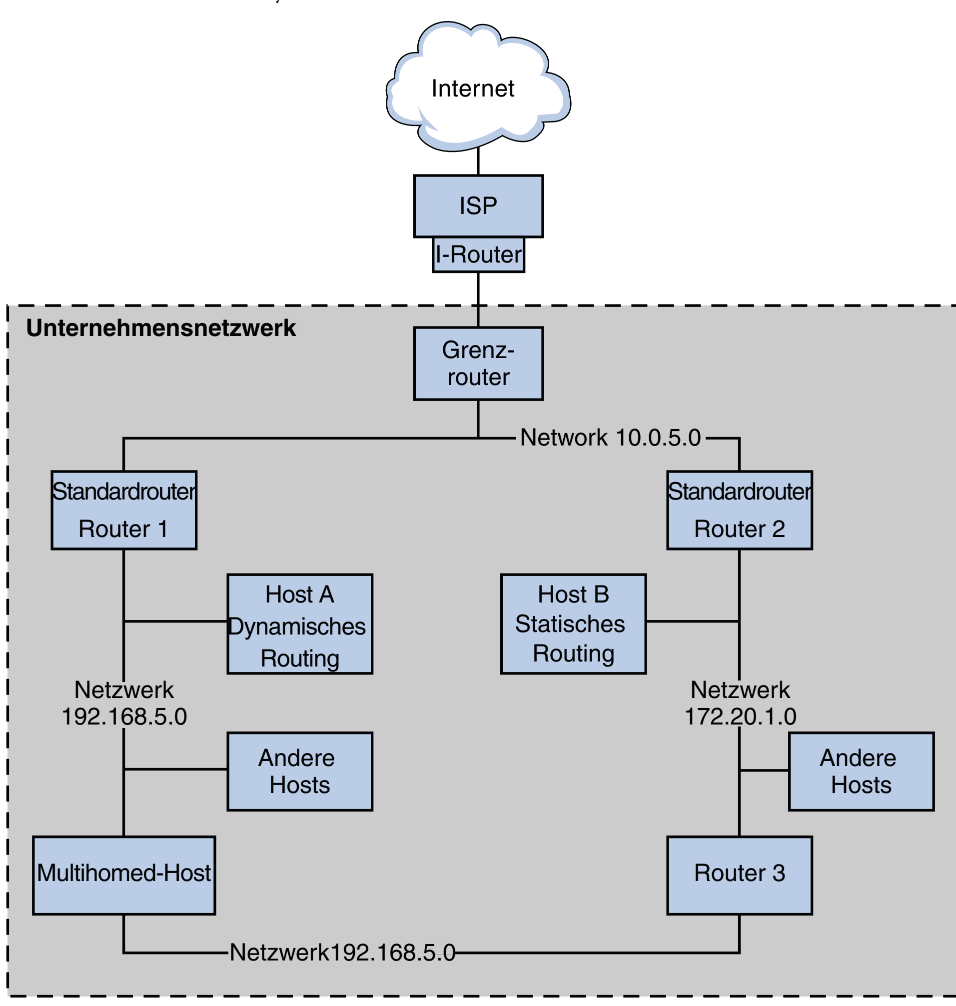
Grenzrouter R1 verbindet das Unternehmensnetzwerk mit einem ISP und schließlich mit dem Internet. Um die Kommunikation zwischen dem Unternehmensnetzwerk und der Außenwelt zu vereinfachen, führt R1 das BGP über die nach außen gerichtete Netzwerkschnittstelle aus. Grenzrouter R5 verbindet Domäne A mit Domäne B. Alle Systeme in Domäne B werden mit RIP als Interior Gateway Protocol verwaltet. Aus diesem Grund muss der Grenzrouter R5 OSPF in der Domäne A zugewandten Schnittstelle und RIP in der Domäne B zugewandten Schnittstelle ausführen.

Weitere Informationen zu den Quagga-Protokollen finden Sie unter Open Solaris Quagga (`http://hub.opensolaris.org/bin/view/Project+quagga/`). Konfigurationsanweisungen für diese Protokolle finden Sie in der Quagga-Dokumentation (`http://quagga.net/docs/docs-info.php`).

Topologie eines autonomen IPv4-Systems

Standorte mit mehreren Routern und Netzwerken verwalten ihre Netzwerktopologie in der Regel als eine Routing-Domäne bzw. als ein *autonomes System (AS)*. Die folgende Abbildung zeigt eine typische Netzwerktopologie, die als ein kleines autonomes System angesehen werden kann. Auf diese Topologie wird im folgenden Abschnitt in Beispielen verwiesen.

ABBILDUNG 5–3 Autonomes System mit mehreren IPv4-Routern



Die Abbildung zeigt ein AS, das in drei lokalen Netzwerke aufgeteilt ist: `10.0.5.0`, `172.20.1.0` und `192.168.5` . Vier Router teilen die Verantwortung für die Paketweiterleitung und das Routing. Das AS umfasst die folgenden Systemtypen:

- *Grenzrouter* verbinden ein AS mit einem externen Netzwerk, z. B. dem Internet. Grenzrouter verbinden externe Netzwerke mit dem IGP, das im lokalen AS ausgeführt wird. Ein Grenzrouter kann ein EGP ausführen, z. B. das Border Gateway Protocol (BGP), um Informationen mit externen Routern auszutauschen, z. B. den Routern beim ISP. In Abbildung 5–3 verbinden die Schnittstellen des Grenzrouters das interne Netzwerk `10.0.5.0` mit einem High-Speed-Router beim Service-Provider.

Informationen zum Konfigurieren eines Grenzrouters und zu BGP finden Sie in der Open Source Quagga-Dokumentation (`http://www.quagga.net/docs/docs-info.php#SEC72`).

Wenn Sie beabsichtigen, Ihr AS mithilfe von BGP mit dem Internet zu verwenden, sollten Sie eine autonome Systemnummer (ASN) von der Internet Registry für Ihr Gebiet beziehen. Regionale Registrierungsbehörden wie die American Registry for Internet Numbers (ARIN) bieten Richtlinien, wie eine ASN bezogen werden kann. Das ARIN Number Resource Policy Manual (`https://www.arin.net/policy/nrpm.html#five`) enthält beispielsweise eine Anleitung zum Beziehen einer ASN für autonome Systeme in den USA und Kanada. Alternativ ist eventuell Ihr ISP in der Lage, eine ASN für Sie zu beziehen.

- *Standard-Router* verwalten Routing-Informationen zu allen Systemen im lokalen Netzwerk. Diese Router führen in der Regel IGPs wie z. B. RIP aus. In Abbildung 5–3 sind die Schnittstellen von Router 1 mit dem internen Netzwerk `10.0.5.0` und dem internen Netzwerk `192.168.5` verbunden. Router 1 dient außerdem als Standard-Router für `192.168.5`. Router 1 verwaltet die Rounting-Informationen aller Systeme in `192.168.5` und leitet an die verbleibenden Router weiter, wie dem Grenzrouter. Die Schnittstellen von Router 2 sind mit dem internen Netzwerk `10.0.5.0` und dem internen Netzwerk `172.20.1` verbunden.

  Ein Beispiel für die Konfiguration eines Standard-Routers finden Sie in Beispiel 5–4.
- *Router zur Paketweiterleitung* leiten Pakete weiter, führen aber keine Routing-Protokolle aus. Dieser Routertyp empfängt Pakete von einer seiner Schnittstellen, die mit einem einzelnen Netzwerk verbunden ist. Diese Pakete werden dann über eine andere Schnittstelle des Routers an ein anderes lokales Netzwerk weitergeleitet. In Abbildung 5–3 ist Router 3 ein Router zur Paketweiterleitung mit Verbindungen zu den Netzwerken `172.20.1` und `192.168.5`.
- *Multihomed-Hosts* verfügen über mindestens zwei Schnittstellen, die mit dem gleichen Netzwerksegment verbunden sind. Ein Multihomed-Host kann Pakete weiterleiten. Dies ist die Standardeinstellung für alle Systeme, die Oracle Solaris ausführen. Abbildung 5–3 zeigt einen Multihomed-Host, dessen zwei Schnittstellen mit dem Netzwerk `192.168.5` verbunden sind. Ein Beispiel für die Konfiguration eines Multihomed-Host finden Sie in Beispiel 5–6.
- *Hosts mit nur einer Schnittstelle* verlassen sich nicht nur zur Paketweiterleitung, sondern auch zum Abrufen von wichtigem Konfigurationsinformationen auf lokale Router. Abbildung 5–3 zeigt Host A im Netzwerk `192.168.5`, in dem dynamisches Routing ausgeführt wird, und Host B im Netzwerk `172.20.1`, in dem statisches Routing ausgeführt wird. Informationen zur Konfiguration eines Hosts zum Ausführen von dynamischem Routing finden Sie unter „So aktivieren Sie das dynamische Routing auf einem Host mit einer Schnittstelle“ auf Seite 140. Informationen zur Konfiguration eines Hosts zum Ausführen von statischem Routing finden Sie unter „So aktivieren Sie statisches Routing auf einem Host mit einer Schnittstelle“ auf Seite 138.

Konfiguration eines IPv4-Routers

Dieser Abschnitt enthält ein Verfahren zur Konfiguration eines IPv4-Routers sowie ein Beispiel. Informationen zur Konfiguration eines IPv6-konformen Routers finden Sie unter „So konfigurieren Sie einen IPv6-konformen Router“ auf Seite 192.

Da ein Router die Schnittstelle zwischen zwei oder mehr Netzwerken darstellt, müssen Sie jeder physikalischen Netzwerkschnittstelle eines Routers einen einmaligen Namen sowie eine IP-Adresse zuweisen. Somit weist jeder Router einen Hostnamen und eine IP-Adresse auf, die seiner primären Netzwerkschnittstelle zugeordnet sind, sowie mindestens einen zusätzlichen einmaligen Namen und eine IP-Adresse für jede zusätzliche Netzwerkschnittstelle.

Sie können auch das folgende Verfahren verwenden, um ein System mit nur einer physikalischen Schnittstelle (standardmäßig ein Host) als Router zu konfigurieren. Sie können ein System mit einer Schnittstelle als Router konfigurieren, wenn das System als Endpunkt einer PPP-Link verwendet wird (siehe „Planning a Dial-up PPP Link“ in *System Administration Guide: Network Services*).

Hinweis – Sie können alle Schnittstellen eines Routers während der Installation von Oracle Solaris konfigurieren. Vollständige Anweisungen hierzu finden Sie im *Oracle Solaris 10 9/10 Installationshandbuch: Grundinstallationen*.

▼ So konfigurieren Sie einen IPv4-Router

Bei den folgenden Anweisungen wird davon ausgegangen, dass Sie nach der Installation Schnittstellen für den Router konfiguriert haben.

Bevor Sie beginnen Nachdem der Router im Netzwerk installiert wurde, konfigurieren Sie ihn für den Betrieb im lokale Dateien-Modus. Dies wird unter „So konfigurieren Sie einen Host für den lokale Dateien-Modus“ auf Seite 109 beschrieben. Diese Konfiguration stellt sicher, dass Router auch dann booten, wenn der Netzwerkkonfigurationsserver heruntergefahren ist.

1. **Nehmen Sie auf dem System, das als Router konfiguriert werden soll, die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Ab Release Solaris 10 1/06 können Sie mit dem Befehl `dladm show-link` feststellen, welche Schnittstellen im Router installiert sind.**

```
# dladm show-link
```

Die folgende Ausgabe des Befehls `dladm show-link` zeigt, dass eine NIC `qfe` mit vier Schnittstellen und zwei `bge`-Schnittstellen im System verfügbar sind.

```
qfe0            type: legacy    mtu: 1500       device: qfe0
qfe1            type: legacy    mtu: 1500       device: qfe1
qfe2            type: legacy    mtu: 1500       device: qfe0
qfe3            type: legacy    mtu: 1500       device: qfe1
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1
```

3. **Prüfen Sie, welche Schnittstellen während der Installation im Router konfiguriert und geplumbt (aktiviert) wurden.**

```
# ifconfig -a
```

Die folgende Beispielausgabe des Befehls `ifconfig -a` zeigt, dass die Schnittstelle `qfe0` während der Installation konfiguriert wurde. Diese Schnittstelle befindet sich im Netzwerk `172.16.0.0`. Die verbleibenden Schnittstellen auf der `qfe`-NIC, `qfe1` - `qfe3`, und die `bge`-Schnittstellen wurden nicht konfiguriert.

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 172.16.26.232 netmask ffff0000 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:15
```

4. **Konfigurieren und plumben Sie eine weitere Schnittstelle.**

`# ifconfig` *interface* `plumb up`

Für `qfe1` geben Sie z. B. Folgendes ein:

```
# ifconfig qfe1 plumb up
```

Hinweis – Schnittstellen, die explizit mit dem Befehl `ifconfig` konfiguriert wurden, behalten ihre Konfiguration nach einem Neustart nicht bei.

---

5. **Weisen Sie der Schnittstelle eine IPv4-Adresse und eine Netzmaske zu.**

Achtung – Sie können einen IPv4-Router zum Empfang seiner IP-Adresse über das DHCP-Protokoll konfigurieren, aber dies wird nur erfahrenen DHCP-Systemadministratoren empfohlen.

`# ifconfig` *interface IPv4-address* `netmask+`*netmask*

Um `qfe1` beispielsweise die IP-Adresse `192.168.84.3` zuzuweisen, führen Sie einen der folgenden Schritte aus:

- Bei der traditionellen IPv4-Notation geben Sie Folgendes ein:

```
# ifconfig qfe1 192.168.84.3 netmask + 255.255.255.0
```

- Bei der CIDR-Notation geben Sie Folgendes ein:

```
# ifconfig qfe1 192.168.84.3/24
```

Das Präfix `/24` weist `qfe1` automatisch die Netzmaske `255.255.255.0` zu. Eine Tabelle der CIDR-Präfixe und deren Netzmaskenäquivalente in der getrennten dezimalen Notation finden Sie in Abbildung 2–2.

6 (Optional) Um sicherzustellen, dass die Schnittstellenkonfiguration auch nach einem Neustart beibehalten wird, erstellen Sie für jede physikalische Schnittstelle eine `/etc/hostname.`*Schnittstelle*-Datei.

Beispielsweise können Sie die Dateien `/etc/hostname.qfe1` und `/etc/hostname.qfe2` erstellen. Dann geben Sie den Hostnamen `timbuktu` in die Datei `/etc/hostname.qfe1` und den Hostnamen `timbuktu-201` in die Datei `/etc/hostname.qfe1` ein. Weitere Informationen zur Konfiguration von einzelnen Schnittstellen finden Sie unter „So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation" auf Seite 159.

Nach dem Erstellen dieser Datei müssen Sie einen Neustart zur Konfiguration durchführen:

```
# reboot -- -r
```

7 Geben Sie den Hostnamen und die IP-Adresse jeder Schnittstelle in die `/etc/inet/hosts`-Datei ein.

Beispiel:

```
172.16.26.232      deadsea        #interface for network 172.16.0.0
192.168.200.20     timbuktu       #interface for network 192.168.200
192.168.201.20     timbuktu-201   #interface for network 192.168.201
192.168.200.9      gobi
192.168.200.10     mojave
192.168.200.110    saltlake
192.168.200.12     chilean
```

Die Schnittstellen `timbuktu` und `timbuktu-201` befinden sich auf dem gleichen System. Denken Sie daran, dass sich die Netzwerkadresse für `timbuktu-201` von der Adresse für die Netzwerkschnittstelle für `timbuktu` unterscheidet. Dieser Unterschied beruht darauf, dass das physikalische Netzwerkmedium des Netzwerks `192.168.201` mit der Netzwerkschnittstelle `timbuktu-201` verbunden ist, während das Medium des Netzwerks `192.168.200` an die Schnittstelle `timbuktu` angeschlossen ist.

8 Unter Solaris 10 11/06 und früheren Releases von Solaris 10 fügen Sie die IP-Adresse und den Hostnamen jeder neuen Schnittstelle in die `/etc/inet/ipnodes`-Datei oder in die entsprechende `ipnodes`-Datenbank ein.

Beispiel:

```
vi /etc/inet/ipnodes
172.16.26.232      deadsea        #interface for network 172.16.0.0
192.168.200.20     timbuktu       #interface for network 192.168.200
192.168.201.20     timbuktu-201   #interface for network 192.168.201
```

9 Ist der Router mit einem Netzwerk verbunden, das über Teilnetze verfügt, geben Sie die Netzwerknummer und die Netzmaske in die `/etc/inet/netmasks`-Datei ein.

- Bei der herkömmlichen IPv4-Adress-Notation wie `192.168.83.0` geben Sie z. B. Folgendes ein:

```
192.168.83.0    255.255.255.0
```

- Bei CIDR-Adressen verwenden Sie die getrennte dezimale Notation für das Präfix im Eintrag der `/etc/inet/netmask`-Datei. Netzwerkpräfixe und deren Entsprechungen in der getrennten dezimalen Notation finden Sie in Abbildung 2–2. Beispielsweise können Sie den folgenden Eintrag in die `/etc/netmasks`-Datei eingeben, um das CIDR-Netzwerkpräfix `192.168.3.0/22` auszudrücken:

```
192.168.3.0 255.255.252.0
```

10 Aktivieren Sie die IPv4-Paketweiterleitung auf dem Router.

Geben Sie einen der folgenden Befehle ein, um die Paketweiterleitung zu aktivieren:

- Verwenden Sie entweder den `routeadm`-Befehl:

```
# routeadm -e ipv4-forwarding -u
```

- Oder verwenden Sie den folgenden Service Management Facility (SMF)-Befehl:

```
# svcadm enable ipv4-forwarding
```

Jetzt kann der Router Pakete über das lokale Netzwerk hinaus weiterleiten. Außerdem unterstützt der Router das *statische Routing*, ein Prozess, bei dem Sie der Routing-Tabelle manuell Routen hinzufügen. Wenn das statische Routing für dieses System verwendet werden soll, ist die Routerkonfiguration abgeschlossen. Sie müssen jedoch die Routen in der Routing-Tabelle des Systems pflegen. Informationen zum Hinzufügen von Routen finden Sie unter „Konfiguration von Routen“ auf Seite 132 und in der Manpage `route(1M)`.

11 (Optional) Starten Sie ein Routing-Protokoll.

Der Routing-Daemon `/usr/sbin/in.routed` aktualisiert automatisch die Routing-Tabelle; ein Prozess, der als *dynamisches Routing* bezeichnet wird. Aktivieren Sie die standardmäßigen IPv4-Routing-Protokolle mit einem der folgenden Verfahren:

- Verwenden Sie entweder den `routeadm`-Befehl:

```
# routeadm -e ipv4-routing -u
```

- Verwenden Sie den folgenden SMF-Befehl zum Starten eines Routing-Protokolls wie z. B. RIP.

```
# svcadm enable route:default
```

  Das dem `in.routed`-Daemon zugewiesene SMF FMRI ist `svc:/network/routing/route`.

Weitere Informationen zum `routeadm`-Befehl finden Sie in der Manpage `routeadm(1M)`.

Beispiel 5–4 Konfiguration des Standard-Routers für ein Netzwerk

Im folgenden Beispiel wird gezeigt, wie Sie ein System mit mehreren Schnittstellen aufrüsten, damit es zu einem Standard-Router wird. Das Ziel besteht darin, den in Abbildung 5–3 gezeigten Router 2 zum Standard-Router für das Netzwerk `172.20.1.0` zu machen. Router 2 enthält zwei verdrahtete Netzwerkverbindungen, eine Verbindung zum Netzwerk `172.20.1.0` und eine weitere zum Netzwerk `10.0.5.0`. Bei diesem Beispiel wird davon ausgegangen, dass der Router im lokale Dateien-Modus betrieben wird, der unter „So konfigurieren Sie einen Host für den lokale Dateien-Modus" auf Seite 109 beschrieben wird.

Nachdem Sie sich als Superuser oder in einer äquivalenten Rolle angemeldet haben, können Sie den Status der Schnittstellen des Systems überprüfen.Ab Solaris 10 1/06 können Sie den Befehl `dladm` wie folgt verwenden:

```
# dladm show-link
ce0             type: legacy    mtu: 1500       device: ce0
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1

# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 172.20.1.10 netmask ffff0000 broadcast 172.20.10.100
        ether 8:0:20:c1:1b:c6
```

Die Ausgabe des Befehls `dladm show-link` zeigt, dass drei Links auf dem System verfügbar sind. Nur die Schnittstelle `ce0` wurde geplumbt (aktiviert). Sie würden jetzt mit der Konfiguration des Standard-Routers beginnen, indem Sie die Schnittstelle `bge0` mit dem Netzwerk `10.0.5.0` verbinden. Dann plumben (aktivieren) Sie die Schnittstelle und sorgen so dafür, dass die Konfiguration auch nach einem Neustart beibehalten wird.

```
# ifconfig bge0 plumb up
# ifconfig bge0 10.0.5.10
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 172.20.1.10 netmask ffff0000 broadcast 172.255.255.255
        ether 8:0:20:c1:1b:c6
bge0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.5.10 netmask ff000000 broadcast 10.255.255.255
        ether 8:0:20:e5:95:c4
 # vi /etc/hostname.bge0
10.0.5.10
255.0.0.0
```

Booten Sie das System, um die neue Konfiguration zu übernehmen:

```
# reboot -- -r
```

Setzen Sie fort, indem Sie die folgenden Netzwerkdatenbanken mit Informationen zur neu geplumbten Schnittstelle und dem Netzwerk konfigurieren, mit dem sie verbunden ist:

```
# vi /etc/inet/hosts
127.0.0.1       localhost
172.20.1.10        router2        #interface for network 172.20.1
10.0.5.10          router2-out    #interface for network 10.0.5
# vi /etc/inet/netmasks
172.20.1.0    255.255.0.0
10.0.5.0      255.0.0.0
```

Abschließend verwenden Sie SMF, um die Paketweiterleitung zu aktivieren und starten dann den `in.routed`-Routing-Daemon.

```
# svcadm enable ipv4-forwarding
# svcadm enable route:default
```

Jetzt sind IPv4-Paketweiterleitung und dynamisches Routing über RIP auf Router 2 aktiviert. Die Standard-Routerkonfiguration für das Netzwerk `172.20.1.0` ist jedoch noch nicht abgeschlossen. Sie müssen noch Folgendes ausführen:

- Ändern Sie jeden Host in `172.10.1.10`, so dass er seine Routing-Informationen vom neuen Standard-Router bezieht. Weitere Informationen hierzu finden Sie unter „So aktivieren Sie statisches Routing auf einem Host mit einer Schnittstelle“ auf Seite 138.
- Definieren Sie in der Routing-Tabelle von Router 2 eine statische Route zum Grenzrouter. Ausführliche Informationen finden Sie unter „Routing-Tabellen und Routing-Typen“ auf Seite 131.

Routing-Tabellen und Routing-Typen

Sowohl Router als auch Hosts pflegen eine *Routing-Tabelle*. Der Routing-Daemon auf jedem System aktualisiert die Tabelle mit allen bekannten Routen. Der Systemkernel liest die Routing-Tabelle ein, bevor Pakete an das lokale Netzwerk weitergeleitet werden. Die Routing-Tabelle enthält die IP-Adressen der Netzwerke, die dem System bekannt sind, einschließlich dem lokalen Standardnetzwerk des Systems. Darüber hinaus führt die Tabelle die IP-Adresse eines Gateway-Systems für jedes bekannte Netzwerk auf. Ein *Gateway* ist ein System, das abgehende Pakete empfangen und einen Hop über das lokale Netzwerk hinaus weiterleiten kann. Im Folgenden ist eine einfache Routing-Tabelle für ein System in einem IPv4-Netzwerk aufgeführt:

```
Routing Table: IPv4
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
default              172.20.1.10          UG       1    532   ce0
224.0.0.0            10.0.5.100           U        1      0   bge0
10.0.0.0             10.0.5.100           U        1      0   bge0
127.0.0.1            127.0.0.1            UH       1     57   lo0
```

Sie können zwei Routing-Arten auf einem Oracle Solaris-System konfigurieren: statisches Routing und dynamisches Routing. Ein System kann entweder mit einer oder mit beiden Routing-Arten konfiguriert werden. Ein System, in dem das *dynamische Routing* umgesetzt

wird, verlässt sich zur Verwaltung der Routing-Tabellen auf Routing-Protokolle, z. B. RIP für IPv4- und RIPng für IPv6-Netzwerke. Ein System, das nur *statisches Routing* ausführt, verlässt sich nicht auf ein Routing-Protokoll zur Angabe der Routing-Informationen und zum Aktualisieren der Routing-Tabelle. Stattdessen müssen Sie die dem System bekannten Routen manuell über den Befehl `route` einpflegen. Weitere Informationen finden Sie in der Manpage `route(1M)`.

Wenn Sie das Routing für das lokale Netzwerk oder ein autonomes System konfigurieren, müssen Sie berücksichtigen, welche Routing-Art auf den jeweiligen Routern und Hosts unterstützt wird.

Die folgende Tabelle zeigt die verschiedenen Routing-Typen und die Netzwerk-Szenarien, in denen die Routing-Typen eingesetzt werden.

Routing-Art	Eignung für
Statisch	Kleine Netzwerke, Hosts, die ihre Routen von einem Standard-Router beziehen und Standard-Router die nur über eine oder zwei Router in den nächsten Hops informiert sein müssen.
Dynamisch	Größere Internetzwerk, Router in lokalen Netzwerken mit vielen Hosts und Hosts in großen autonomen Systemen. Das dynamische Routing ist die beste Wahl für Systeme in den meisten Netzwerken.
Kombination von statischem und dynamischem Routing	Router, die eine Verbindung zu einem Netzwerk mit statischem Routing und einem Netzwerk mit dynamischem Routing herstellen sowie Grenzrouter, die autonome Systeme mit externen Netzwerken verbinden. Eine Kombination aus statischem und dynamischem Routing auf einem System ist gängige Praxis.

Das in Abbildung 5–3 gezeigte autonome System kombiniert sowohl statisches als auch dynamisches Routing.

Konfiguration von Routen

Zum Umsetzen des dynamischen Routings für ein IPv4-Netzwerk verwenden Sie den Befehl `routeadm` oder `svcadm`, um den `in.routed`-Routing-Daemon zu starten. Anweisungen hierzu finden Sie unter „So konfigurieren Sie einen IPv4-Router“ auf Seite 126. Das dynamische Routing ist die bevorzugte Strategie für die meisten Netzwerke und autonomen Systeme. Eventuell erfordern Ihre Netzwerktopologie oder ein bestimmtes System in Ihrem Netzwerk jedoch statisches Routing. In diesem Fall müssen Sie die Routing-Tabelle des Systems manuell bearbeiten, um die bekannten Route zum Gateway einzupflegen. Das nächste Verfahren zeigt, wie eine statische Route hinzugefügt wird.

Hinweis – Zwei Routen zum gleichen Ziel führen nicht automatisch dazu, dass das System einen Lastenausgleich oder ein Failover ausführt. Wenn Sie diese Fähigkeiten benötigen, verwenden Sie IPMP. Dies wird in Kapitel 30, „Einführung in IPMP (Übersicht)" beschrieben.

So fügen Sie einer Routing-Tabelle eine statische Route hinzu

1. **Zeigen Sie den aktuellen Status der Routing-Tabelle an.**

   Verwenden Sie Ihr normales Benutzerkonto, und geben Sie den folgenden `netstat`-Befehl ein:

   ```
   % netstat -rn
   ```

   Der Befehl sollte eine Ausgabe ähnlich der Folgenden erzeugen:

   ```
   Routing Table: IPv4
     Destination           Gateway           Flags  Ref   Use   Interface
   -------------------- -------------------- ----- ----- ------ ---------
   192.168.5.125        192.168.5.10          U      1   5879   ipge0
   224.0.0.0            198.168.5.10          U      1  0       ipge0
   default              192.168.5.10          UG     1  91908
   127.0.0.1            127.0.0.1             UH     1  811302   lo0
   ```

2. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

3. **(Optional) Löschen Sie die vorhandenen Einträge aus der Routing-Tabelle.**

   ```
   # route flush
   ```

4. **Fügen Sie eine Route hinzu, die auch nach dem Neustart eines Systems beibehalten wird.**

   `# route -p add -net` *network-address* `-gateway` *gateway-address*

`-p`	Erstellt eine Route, die auch nach dem Neustart eines Systems beibehalten wird. Wenn diese Route nur für die aktuelle Sitzung gelten soll, verwenden Sie die Option `-p` nicht.
`add`	Gibt an, dass Sie die folgende Route hinzufügen möchten.
`-net` *Netzwerkadresse*	Gibt an, dass die Route beim Netzwerk mit der Adresse in *Netzwerkadresse* endet.
`-gateway` *Gatewayadresse*	Gibt an, dass das Gateway-System für die angegebene Route die IP-Adresse *Gatewayadresse* hat.

Beispiel 5–5 Hinzufügen einer statischen Route zu einer Routing-Tabelle

Das folgende Beispiel zeigt, wie Sie einem System eine statische Route hinzufügen. Das System ist Router 2, der Standard-Router für das Netzwerk `172.20.1.0` wird in Abbildung 5–3 gezeigt. In Beispiel 5–4 ist Router 2 für das dynamische Routing konfiguriert. Damit Router 2 besser als Standard-Router für die Hosts im Netzwerk `172.20.1.0` arbeiten kann, benötigt er eine statische Route zum Grenzrouter des AS, `10.0.5.150` .

Zum Anzeigen der Routing-Tabelle auf Router 2 geben Sie Folgendes ein:

```
# netstat -rn
Routing Table: IPv4
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
default              172.20.1.10          UG        1    249 ce0
224.0.0.0            172.20.1.10          U         1      0 ce0
10.0.5.0             10.0.5.20            U         1     78 bge0
127.0.0.1            127.0.0.1            UH        1     57 lo0
```

Die Routing-Tabelle zeigt zwei Routen an, die Router 2 bekannt sind. Die Standardroute verwendet die Schnittstelle `172.20.1.10` von Router 2 als Gateway. Die zweite Route `10.0.5.0` wurde vom `in.routed`-Daemon ermittelt, der auf Router 2 läuft. Das Gateway für diese Route ist Router 1 und besitzt die IP-Adresse `10.0.5.20` .

Um eine zweite Route zum Netzwerk `10.0.5.0` hinzuzufügen, das seinen Gateway als Grenzrouter verwendet, geben Sie Folgendes ein:

```
# route -p add -net 10.0.5.0/24 -gateway 10.0.5.150/24
add net 10.0.5.0: gateway 10.0.5.150
```

Jetzt enthält die Routing-Tabelle eine Route für den Grenzrouter mit der IP-Adresse `10.0.5.150/24`.

```
# netstat -rn
Routing Table: IPv4
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
default              172.20.1.10          UG        1    249 ce0
224.0.0.0            172.20.1.10          U         1      0 ce0
10.0.5.0             10.0.5.20            U         1     78 bge0
10.0.5.0             10.0.5.150           U         1    375 bge0
127.0.0.1            127.0.0.1            UH        1     57 lo0
```

Konfiguration von Multihomed-Hosts

Unter Oracle Solaris wird ein System mit mehreren Schnittstellen als ein *Multihomed-Host* bezeichnet. Ein Multihomed-Host leitet keine IP-Pakete weiter. Sie können einen

Multihomed-Host jedoch so konfigurieren, dass er Routing-Protokolle ausführt. In der Regel werden die folgenden Systemarten als Multihomed-Hosts konfiguriert:

- NFS-Server, insbesondere die Server, die als große Datencenter fungieren, können an mehrere Netzwerke angehängt werden, damit Dateien gemeinsam von einem großen Benutzerpool genutzt werden können. Diese Server müssen keine Routing-Tabellen pflegen.
- Datenbankserver können über mehrere Netzwerkschnittstellen verfügen, um einem großen Benutzerpool Ressourcen bereitstellen zu können (wie NFS-Server).
- Firewall-Gateways sind Systeme, die eine Verbindung zwischen einem Firmennetzwerk und einem öffentlichen Netzwerk wie z. B. dem Internet herstellen. Firewalls werden von Administratoren als Sicherheitsmaßnahme eingerichtet. Wenn ein Host als Firewall konfiguriert ist, lässt er keine Pakete zwischen den Netzwerken passieren, die an die Schnittstellen des Hosts angeschlossen sind. Dennoch kann der Host für autorisierte Benutzer standardmäßige TCP/IP-Services, z. B. `ssh` bereitstellen.

Hinweis – Wenn Multihomed-Hosts verschiedene Firewalltypen an ihren Schnittstellen aufweisen, müssen Sie darauf achten, die Hosts-Pakete nicht unabsichtlich zu unterbrechen. Dieses Problem tritt insbesondere bei statusbehafteten Firewalls auf. Eine Lösung könnte das Konfigurieren einer statusfreien Firewall sein. Weitere Informationen zu Firewalls finden Sie unter „Firewall Systems“ in *System Administration Guide: Security Services* oder in der Dokumentation Ihrer Firewall.

▼ So erstellen Sie einen Multihomed-Host

1. **Nehmen Sie auf dem künftigen Multihomed-Host die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Konfigurieren und plumben (aktivieren) Sie jede zusätzliche Netzwerkschnittstelle, die nicht während der Installation von Oracle Solaris konfiguriert wurde.**

   Lesen Sie dazu „So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation“ auf Seite 159.

3. **Vergewissern Sie sich, dass die IP-Weiterleitung am Multihomed-Host nicht aktiviert ist.**

```
# routeadm
```

Mit dem Befehl `routeadm` ohne zusätzliche Optionen rufen Sie den Status der Routing-Daemons ab. Die folgende Ausgabe des `routeadm`-Befehls zeigt, dass die IPv4-Weiterleitung aktiviert ist:

```
   Configuration   Current              Current
                     Option   Configuration       System State
---------------------------------------------------------------
               IPv4 routing   disabled            disabled
               IPv6 routing   disabled            disabled
            IPv4 forwarding   enabled             disabled
            IPv6 forwarding   disabled            disabled

            Routing services   "route:default ripng:default"
```

4 Deaktivieren Sie die Paketweiterleitung, sofern diese auf dem System aktiviert ist.

Verwenden Sie einen der folgenden Befehle:

- Beim `routeadm`-Befehl geben Sie Folgendes ein:

  ```
  # routeadm -d ipv4-forwarding -u
  ```

- Für SMF geben Sie Folgendes ein:

  ```
  # svcadm disable ipv4-forwarding
  ```

5 (Optional) Aktivieren Sie das dynamische Routing für den Multihomed-Host.

Geben Sie einen der folgenden Befehle ein, um den `in.routed`-Daemon zu aktivieren:

- Beim `routeadm`-Befehl geben Sie Folgendes ein:

  ```
  # routeadm -e ipv4-routing -u
  ```

- Für SMF geben Sie Folgendes ein:

  ```
  # svcadm enable route:default
  ```

Beispiel 5–6 Konfiguration eines Multihomed-Host

Im folgenden Beispiel wird gezeigt, wie Sie den in Abbildung 5–3 vorgestellten Multihomed-Host konfigurieren. In diesem Beispiel lautet der Hostname des Systems `hostc`. Dieser Host verfügt über zwei Schnittstellen, die beide mit dem Netzwerk `192.168.5.0` verbunden sind.

Zu Beginn zeigen Sie den Status der Systemschnittstellen an.

```
# dladm show-link
hme0           type: legacy    mtu: 1500       device: hme0
qfe0           type: legacy    mtu: 1500       device: qfe0
qfe1           type: legacy    mtu: 1500       device: qfe1
qfe2           type: legacy    mtu: 1500       device: qfe2
qfe3           type: legacy    mtu: 1500       device: qfe3
# ifconfig -a
```

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 192.168.5.82 netmask ff000000 broadcast 192.255.255.255
      ether 8:0:20:c1:1b:c6
```

Der `dladm show-link`-Befehl meldet, dass `hostc` über zwei Schnittstellen mit insgesamt fünf möglichen Links verfügt. Jedoch wurde nur `hme0` geplumbt (aktiviert). Um `hostc` als einen Multihomed-Host zu konfigurieren, müssen Sie `qfe0` oder einen anderen Link auf der NIC `qfe` hinzufügen. Zunächst verbinden Sie die Schnittstelle `qfe0` mit dem Netzwerk `192.168.5.0`. Dann plumben (aktivieren) Sie die Schnittstelle `qfe0` und sorgen so dafür, dass die Schnittstellenkonfiguration auch nach einem Neustart beibehalten wird.

```
# ifconfig qf0 plumb up
# ifconfig qfe0 192.168.5.85
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.5.82 netmask ff0000 broadcast 192.255.255.255
        ether 8:0:20:c1:1b:c6
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.5.85 netmask ff000000 broadcast 192.255.255.255
        ether 8:0:20:e1:3b:c4
 # vi /etc/hostname.qfe0
192.168.5.85
255.0.0.0
```

Booten Sie das System neu, um die Konfiguration zu übernehmen:

```
# reboot -- -r
```

Als Nächstes fügen Sie die Schnittstelle `qfe0` zur `hosts` -Datenbank hinzu:

```
# vi /etc/inet/hosts
127.0.0.1           localhost
192.168.5.82        host3    #primary network interface for host3
192.168.5.85        host3-2  #second interface
```

Dann prüfen Sie den Status der Paketweiterleitung und des Routings auf `host3`:

```
# routeadm
              Configuration   Current              Current
                     Option   Configuration        System State
---------------------------------------------------------------
               IPv4 routing   enabled              enabled
               IPv6 routing   disabled             disabled
            IPv4 forwarding   enabled              enabled
            IPv6 forwarding   disabled             disabled

           Routing services   "route:default ripng:default"
```

Der routeadm-Befehl meldet, dass das dynamische Routing über den in.routed-Daemon und die Paketweiterleitung derzeit aktiviert sind. Die Paketweiterleitung muss jedoch deaktiviert sein:

```
# svcadm disable ipv4-forwarding
```

Sie können die Paketweiterleitung auch mit den routeadm-Befehlen deaktivieren. Lesen Sie dazu „So erstellen Sie einen Multihomed-Host" auf Seite 135 Nachdem die Paketweiterleitung deaktiviert wurde, wird host3 zu einem Multihomed-Host.

Konfiguration des Routings auf Systemen mit einer Schnittstelle

Hosts mit einer Schnittstelle müssen eine Form des Routings implementieren. Wenn der Host seine Routen von einem oder mehreren lokalen Standard-Routern bezieht, müssen Sie den Host zur Verwendung des statischen Routings konfigurieren. Andernfalls wird dynamisches Routing für den Host empfohlen. Die folgenden Verfahren enthalten die Anweisungen zum Umsetzen beider Routing-Arten.

▼ So aktivieren Sie statisches Routing auf einem Host mit einer Schnittstelle

Mit dem folgenden Verfahren wird statisches Routing auf einem Host mit einer Schnittstelle konfiguriert. Hosts, die statisches Routing verwenden, führen kein dynamisches Routing-Protokoll wie z. B. RIP aus. Stattdessen muss sich der Host auf die Services eines Standard-Routers für Routing-Informationen verlassen. Die Abbildung „Topologie eines autonomen IPv4-Systems" auf Seite 123 zeigt verschiedene Standard-Router und deren Client-Hosts. Wenn Sie den Namen eines Standard-Routers bei der Installation eines bestimmten Hosts angegeben haben, wurde das statische Routing bereits auf diesem Host konfiguriert.

Hinweis – Sie können auch das folgende Verfahren verwenden, um statisches Routing auf einem Multihomed-Host zu konfigurieren.

Informationen zur /etc/defaultrouter-Datei finden Sie unter „/etc/defaultrouter-Datei" auf Seite 255. Informationen zum statischen Routing und der Routing-Tabelle finden Sie unter „Routing-Tabellen und Routing-Typen" auf Seite 131.

1. **Nehmen Sie auf einem Host mit einer Schnittstelle die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Prüfen Sie, ob die `/etc/defaultrouter`-Datei auf dem Host vorhanden ist.**

   ```
   # cd /etc
   # ls | grep defaultrouter
   ```

3. **Öffnen Sie einen Texteditor, um die `/etc/defaultrouter`-Datei zu erstellen oder zu bearbeiten.**

4. **Fügen Sie einen Eintrag für den Standard-Router hinzu.**

   ```
   # vi  /etc/defaultrouter
   router-IP
   ```

   Router-IP steht für die IP-Adresse des Standard-Routers, den der Host verwenden soll.

5. **Prüfen Sie, ob Routing und Paketweiterleitung auf dem Host ausgeführt werden oder nicht.**

   ```
   # routeadm
      Configuration   Current              Current
                       Option   Configuration        System State
   ---------------------------------------------------------------
                  IPv4 routing   disabled             disabled
                  IPv6 routing   disabled             disabled
               IPv4 forwarding   disabled            disabled
               IPv6 forwarding   disabled             disabled

              Routing services   "route:default ripng:default"
   ```

6. **Fügen Sie einen Eintrag für den Standard-Router in die lokale `/etc/inet/hosts`-Datei ein.**

   Informationen zur Konfiguration der `/etc/inet/hosts`-Datei finden Sie unter „So ändern Sie die IPv4-Adresse und andere Netzwerkkonfigurationsparameter" auf Seite 114.

Beispiel 5–7 Konfiguration eines Standard-Routers und des statischen Routings für einen Host mit einer Schnittstelle

Das folgende Beispiel zeigt, wie statisches Routing für `hostb`, einem Host mit einer Schnittstelle im Netzwerk `172.20.1.0`, konfiguriert wird. Das Netzwerk wird in Abbildung 5–3 gezeigt. `hostb` muss Router 2 als Standard-Router verwenden.

Als Erstes melden Sie sich als Superuser bei `hostb` an oder nehmen eine entsprechende Rolle an. Dann prüfen Sie, ob die `/etc/defaultrouter`-Datei auf dem Host vorhanden ist:

```
# cd /etc
# ls | grep defaultrouter
```

Keine Antwort von `grep` deutet darauf hin, dass Sie die `/etc/defaultrouter`-Datei erstellen müssen.

```
# vi /etc/defaultrouter
172.20.1.10
```

Der Eintrag in der `/etc/defaultrouter`-Datei ist die IP-Adresse der Schnittstelle auf Router 2, die mit dem Netzwerk `172.20.1.0` verbunden ist. Als Nächstes prüfen Sie, ob Paketweiterleitung oder Routing derzeit auf dem Host aktiviert sind.

```
# routeadm
   Configuration   Current              Current
                     Option   Configuration        System State
---------------------------------------------------------------
               IPv4 routing   disabled             disabled
               IPv6 routing   disabled             disabled
            IPv4 forwarding   enabled              enabled
            IPv6 forwarding   disabled             disabled

           Routing services   "route:default ripng:default"
```

Die Paketweiterleitung ist auf diesem Host aktiviert. Deaktivieren Sie die Paketweiterleitung wie folgt:

```
# svcadm disable ipv4-forwarding
```

Abschließend stellen Sie sicher, dass die `/etc/inet/hosts`-Datei auf dem Host einen Eintrag für den neuen Standard-Router enthält.

```
# vi /etc/inet/hosts
127.0.0.1           localhost
172.20.1.18         host2    #primary network interface for host2
172.20.1.10         router2  #default router for host2
```

So aktivieren Sie das dynamische Routing auf einem Host mit einer Schnittstelle

Dynamisches Routing stellt den einfachsten Weg dar, das Routing auf einem Host zu verwalten. Hosts, die dynamisches Routing verwenden, führen die Routing-Protokolle aus, die vom `in.routed`-Daemon für IPv4 oder dem `in.ripngd`-Daemon für IPv6 zur Verfügung gestellt werden. Mit dem folgenden Verfahren aktivieren Sie das dynamische IPv4-Routing auf einem Host mit einer Schnittstelle. Weitere Informationen zum dynamischen Routing finden Sie unter „Paketweiterleitung und Routing bei IPv4-Netzwerken“ auf Seite 119.

1 **Nehmen Sie auf dem Host die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 **Prüfen Sie, ob die `/etc/defaultrouter`-Datei vorhanden ist.**

```
# cd /etc
# ls | grep defaultrouter
```

3 **Wenn die `/etc/defaultrouter`-Datei vorhanden ist, löschen Sie alle darin enthaltenen Einträge.**

Eine leere `/etc/defaultrouter`-Datei zwingt den Host, dynamisches Routing auszuführen.

4 **Prüfen Sie, ob Paketweiterleitung und Routing auf dem Host aktiviert sind.**

```
# routeadm
   Configuration   Current              Current
                    Option   Configuration       System State
---------------------------------------------------------------
              IPv4 routing   disabled            disabled
              IPv6 routing   disabled            disabled
           IPv4 forwarding   enabled             enabled
           IPv6 forwarding   disabled            disabled

          Routing services   "route:default ripng:default"
```

5 **Wenn die Paketweiterleitung aktiviert ist, deaktivieren Sie sie.**

Verwenden Sie einen der folgenden Befehle:

- Beim `routeadm`-Befehl geben Sie Folgendes ein:

  ```
  # routeadm -d ipv4-forwarding -u
  ```
- Für SMF geben Sie Folgendes ein:

  ```
  # svcadm disable ipv4-forwarding
  ```

6 **Aktivieren Sie die Routing-Protokolle auf dem Host.**

Verwenden Sie einen der folgenden Befehle:

- Beim `routeadm`-Befehl geben Sie Folgendes ein:

  ```
  # routeadm -e ipv4-routing -u
  ```
- Für SMF geben Sie Folgendes ein:

  ```
  # svcadm enable route:default
  ```

Jetzt ist das dynamische IPv4-Routing aktiviert. Die Routing-Tabelle des Hosts wird vom `in.routed`-Daemon dynamisch gepflegt.

Beispiel 5–8 Ausführen des dynamischen Routings auf einem Host mit einer Schnittstelle

Das folgende Beispiel zeigt, wie das dynamische Routing für `hosta`, einem Host mit einer Schnittstelle im Netzwerk `192.168.5.0`, konfiguriert wird. Das Netzwerk wird in Abbildung 5–3 gezeigt. `hosta` verwendet derzeit Router 1 als Standard-Router. Jetzt muss `hosta` jedoch zum Ausführen des dynamischen Routings konfiguriert werden.

Als Erstes melden Sie sich als Superuser bei `hosta` an oder nehmen eine entsprechende Rolle an. Dann prüfen Sie, ob die `/etc/defaultrouter`-Datei auf dem Host vorhanden ist:

```
# cd /etc
# ls | grep defaultrouter
defaultrouter
```

Die Antwort von `grep` deutet darauf hin, dass eine `/etc/defaultrouter`-Datei für `hosta` vorhanden ist.

```
# vi /etc/defaultrouter
192.168.5.10
```

Die Datei besitzt den Eintrag `192.168.5.10` (die IP-Adresse für Router 1). Zum Aktivieren des statischen Routing müssen Sie diesen Eintrag löschen. Als Nächstes überprüfen Sie, ob Paketweiterleitung und Routing bereits für den Host aktiviert sind.

```
# routeadm   Configuration   Current             Current
                    Option   Configuration        System State
---------------------------------------------------------------
              IPv4 routing   disabled             disabled
              IPv6 routing   disabled             disabled
           IPv4 forwarding   disabled             disabled
           IPv6 forwarding   disabled             disabled

          Routing services   "route:default ripng:default"
```

Sowohl Routing als auch Paketweiterleitung sind für `hosta` deaktiviert. Aktivieren Sie das Routing, um die Konfiguration des dynamischen Routings für `hosta` abzuschließen:

```
# svcadm enable route:default
```

Überwachen undModifizieren der Transportschichtservices

Die Transportschichtprotokolle TCP, SCTP und UDP sind Teil des standardmäßigen Oracle Solaris-Pakets. Zur ordnungsgemäßen Ausführung dieser Protokolle ist in der Regel kein Benutzereingriff erforderlich. Dennoch können Umstände an Ihrem Standort es erfordern, die über Transportschichtprotokolle ausgeführten Services zu protokollieren oder zu bearbeiten. Anschließend müssen Sie die Profile für diese Services mithilfe der Service Management Facility

(SMF) ändern. Die SMF wird in Kapitel 18, „Managing Services (Overview)" in *System Administration Guide: Basic Administration* erläutert.

Der `inetd`-Daemon ist für das Starten der Internet-Standardservices beim Booten eines Systems verantwortlich. Diese Services umfassen Anwendungen, die TCP, SCTP oder UDP als Transportschichtprotokoll verwenden. Sie können entweder die vorhandenen Internet-Services ändern oder mithilfe der SMF-Befehle neue Services hinzufügen. Weitere Informationen zum `inetd`-Daemon finden Sie unter „`inetd` Internet Services-Daemon" auf Seite 263.

Vorgänge, die Transportschichtprotokolle erfordern, sind z. B.:

- Das Protokollieren aller eingehenden TCP-Verbindungen
- Das Hinzufügen von Services, die über ein Transportschichtprotokoll ausgeführt werden, z. B. mit SCTP
- Das Konfigurieren der TCP-Wrappers Facility für die Zugangskontrolle

Ausführliche Informationen zum `inetd`-Daemon finden Sie in der Manpage `inetd`(1M).

▼ So protokollieren Sie die IP-Adressen aller eingehenden TCP-Verbindungen

1 Nehmen Sie auf dem lokalen System die Rolle eines Netzwerkmanagers an, oder melden Sie sich als Superuser an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Aktivieren Sie die TCP-Verfolgung für alle Services, die vom `inetd`-Daemon verwaltet werden.

```
# inetadm -M tcp_trace=TRUE
```

▼ So fügen Sie Services hinzu, die das SCTP-Protokoll verwenden

Das SCTP-Transportprotokoll stellt den Protokollen auf der Anwendungsschicht Services ähnlich dem TCP bereit. SCTP ermöglicht jedoch die Kommunikation zwischen zwei Systemen, von denen entweder eines oder beide Multihomed-Hosts sein können. Die SCTP-Verbindung wird als *Assoziation* bezeichnet. Bei einer Assoziation teilt eine Anwendung die zu übertragenden Daten in einen oder mehrere Datenströme oder *Mehrfach-Datenströme* (multi-streamed) auf. Eine SCTP-Verbindung kann zu Endpunkten mit mehreren IP-Adressen

führen, wodurch diese Verbindungsart insbesondere für Telefonieanwendungen wichtig ist. Wenn IP Filter oder IPsec an Ihrem Standort eingesetzt werden, müssen die Multihoming-Fähigkeiten von SCTP in die Sicherheitsbetrachtungen einbezogen werden. Einige dieser Überlegungen sind in der Manpage `sctp`(7P) beschrieben.

SCTP ist standardmäßig in Oracle Solaris enthalten und erfordert keine zusätzliche Konfiguration. Eventuell müssen Sie jedoch bestimmte Services auf der Anwendungsschicht zur Verwendung von SCTP konfigurieren. Einige Beispielanwendungen sind `echo` und `discard`. Im folgenden Verfahren wird gezeigt, wie Sie einen echo-Service hinzufügen, der ein SCTP 1:1-Socket verwendet.

Hinweis – Darüber hinaus können Sie das folgende Verfahren verwenden, um Services für die Transportschichtprotokolle TCP und UDP hinzuzufügen.

In der folgenden Aufgabe wird gezeigt, wie Sie einen SCTP `inet`-Service hinzufügen, der vom `inetd`-Daemon für das SMF-Repository verwaltet wird. Dann wird in der Aufgabe gezeigt, wie der Service mit den Befehlen der Service Management Facility (SMF) hinzugefügt wird.

- Informationen zu den SMF-Befehlen finden Sie unter „SMF Command-Line Administrative Utilities“ in *System Administration Guide: Basic Administration*.
- Syntaktische Informationen finden Sie in den Manpages für die SMF-Befehle, die in diesem Verfahren genannt werden.
- Ausführliche Informationen zu SMF finden Sie in der Manpage `smf`(5).

Bevor Sie beginnen Bevor Sie das folgende Verfahren ausführen, erstellen Sie eine Manifestdatei für den Service. In dem Verfahren wird ein Manifest für den `echo`-Service mit der Bezeichnung `echo.sctp.xml` als Beispiel verwendet.

1 Melden Sie sich mit einem Benutzerkonten, das über Schreibrechte für Systemdateien verfügt, beim lokalen System an.

2 Bearbeiten Sie die `/etc/services`-Datei und fügen Sie eine Definition für den neuen Service hinzu.

Verwenden Sie bei der Definition des Service die folgende Syntax:

service-name |*port/protocol* | *aliases*

3 Fügen Sie den neuen Service hinzu.

Wechseln Sie in das Verzeichnis, in dem das Manifest gespeichert ist, und geben Sie Folgendes ein:

```
# cd dir-name
# svccfg import service-manifest-name
```

Die vollständige Syntax des `svccfg`-Befehls finden Sie in der Manpage `svccfg`(1M).

Angenommen, Sie möchten einen neuen SCTP `echo`-Service mithilfe des Manifests `echo.sctp.xml` hinzufügen, das momentan im Verzeichnis `service.dir` gespeichert ist. In diesem Fall geben Sie Folgendes ein:

```
# cd service.dir
# svccfg import echo.sctp.xml
```

4 **Prüfen Sie, ob das Servicemanifest hinzugefügt wurde:**

`# svcs` *FMRI*

Als *FMRI*-Argument verwenden Sie den Fault Managed Resource Identifier (FMRI) des Servicemanifests. Für den SCTP `echo`-Service verwenden Sie beispielsweise den folgenden Befehl:

```
# svcs svc:/network/echo:sctp_stream
```

Dieser Befehl sollte eine Ausgabe ähnlich der Folgenden erzeugen:

```
    STATE          STIME    FMRI
disabled       16:17:00 svc:/network/echo:sctp_stream
```

Ausführliche Informationen zum `svcs`-Befehl finden Sie in der Manpage `svcs`(1).

Die Ausgabe deutet darauf hin, dass das neue Servicemanifest derzeit deaktiviert ist.

5 **Listen Sie die Eigenschaften des Services auf, um festzustellen, ob Sie Änderungen vornehmen müssen.**

`# inetadm -l` *FMRI*

Ausführliche Informationen zum `inetadm`-Befehl finden Sie in der Manpage `inetadm`(1M).

Für den SCTP `echo`-Service geben Sie z. B. Folgendes ein:

```
# inetadm -l svc:/network/echo:sctp_stream
SCOPE    NAME=VALUE
             name="echo"
             endpoint_type="stream"
             proto="sctp"
             isrpc=FALSE
             wait=FALSE
             exec="/usr/lib/inet/in.echod -s"
         .
         .
         default  tcp_trace=FALSE
           default  tcp_wrappers=FALSE
```

6 **Aktivieren Sie den neuen Service:**

`# inetadm -e` *FMRI*

7 Prüfen Sie, ob der Service aktiviert wurde:

Für den neuen echo-Service geben Sie z. B. Folgendes ein:

```
# inetadm | grep sctp_stream
.
.
    enabled   online         svc:/network/echo:sctp_stream
```

Beispiel 5–9 Hinzufügen eines Services, der das SCTP-Transportprotokoll verwendet

Im folgenden Beispiel werden die Befehle und Dateieinträge vorgestellt, mit denen Sie dafür sorgen, dass der echo-Service das SCTP-Transportschichtprotokoll verwendet.

```
$ cat /etc/services
.
.
echo            7/tcp
echo            7/udp
echo            7/sctp

# cd service.dir

    # svccfg import echo.sctp.xml

# svcs network/echo*
    STATE          STIME    FMRI
    disabled       15:46:44 svc:/network/echo:dgram
    disabled       15:46:44 svc:/network/echo:stream
    disabled       16:17:00 svc:/network/echo:sctp_stream

# inetadm -l svc:/network/echo:sctp_stream
    SCOPE    NAME=VALUE
             name="echo"
             endpoint_type="stream"
             proto="sctp"
             isrpc=FALSE
             wait=FALSE
             exec="/usr/lib/inet/in.echod -s"
             user="root"
    default  bind_addr=""
    default  bind_fail_max=-1
    default  bind_fail_interval=-1
    default  max_con_rate=-1
    default  max_copies=-1
    default  con_rate_offline=-1
    default  failrate_cnt=40
    default  failrate_interval=60
    default  inherit_env=TRUE
    default  tcp_trace=FALSE
    default  tcp_wrappers=FALSE

# inetadm -e svc:/network/echo:sctp_stream

# inetadm | grep echo
    disabled  disabled       svc:/network/echo:stream
```

```
disabled  disabled      svc:/network/echo:dgram
enabled   online        svc:/network/echo:sctp_stream
```

▼ So verwenden Sie TCP-Wrapper zur Kontrolle des Zugriffs auf TCP-Services

Das `tcpd`-Programm implementiert *TCP-Wrapper*. TCP-Wrapper stellen eine Sicherheitsmaßnahme für Service-Daemons wie `ftpd` dar, indem sie zwischen dem Daemon und den eingehenden Serviceanforderungen stehen. TCP-Wrapper protokollieren erfolgreiche und nicht erfolgreiche Verbindungsversuche. Darüber hinaus stellen TCP-Wrapper eine Zugriffskontrolle bereit, indem sie eine Verbindung abhängig vom Ursprung der Anforderung zulassen oder verweigern. Sie verwenden TCP-Wrapper zum Schutz von Daemons wie z. B. SSH, Telnet und FTP. Auch die Anwendung `sendmail` kann TCP-Wrapper verwenden, wie unter „Support for TCP Wrappers From Version 8.12 of sendmail“ in *System Administration Guide: Network Services* beschrieben.

1. **Nehmen Sie auf dem lokalen System die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Aktivieren Sie die TCP-Wrapper.**

   ```
   # inetadm -M tcp_wrappers=TRUE
   ```

3. **Konfigurieren Sie die Zugriffskontroll-Richtlinie der TCP-Wrapper gemäß der Beschreibung in der Manpage `hosts_access`(3)**

   Diese Manpage finden Sie im Verzeichnis `/usr/sfw/man` auf der SFW CD-ROM, die zusammen mit der Oracle Solaris CD-ROM ausgeliefert wird.

Verwalten der Schnittstellen in Solaris 10 3/05

In diesem Abschnitt sind die folgenden Aufgaben zur Verwaltung von physikalischen Schnittstellen enthalten:

- Hinzufügen von physikalischen Schnittstellen nach der Systeminstallation
- Hinzufügen eines virtuellen lokalen Netzwerks (VLAN) zu einem Netzwerkadapter

Neuerungen in diesem Abschnitt

Dieser Abschnitt enthält ausschließlich Informationen zur Konfiguration von Schnittstellen für Benutzer von Solaris 10 3/05. Wenn Sie ein Update auf Oracle Solaris 10 verwenden, lesen Sie Chapter 6, Verwalten von Netzwerkschnittstellen (Aufgaben). Eine vollständige Liste der neuen Oracle Solaris-Funktionen und eine Beschreibung der Oracle Solaris-Versionen finden Sie im Handbuch *Neuerungen in Oracle Solaris 9 10/10*.

Konfiguration physikalischer Schnittstellen unter Solaris 10 3/05

Ein Oracle Solaris-basiertes System verwendet in der Regel zwei Arten von Schnittstellen: physikalisch und logisch. *Physikalische Schnittstellen* bestehen aus einem Softwaretreiber und einem Anschluss, über den sie eine Verbindung mit dem Netzwerkmedium, z. B. ein Ethernet-Kabel, herstellen. *Logische Schnittstellen* sind logisch in vorhandenen physikalischen Schnittstellen konfiguriert, z. B. Schnittstellen, die für Tunnel oder mit IPv6-Adressen konfiguriert wurden. In diesem Abschnitt wird beschrieben, wie Sie physikalische Schnittstellen nach der Installation konfigurieren. Anweisungen zur Konfiguration von logischen Schnittstellen sind bei den Aufgaben für Funktionen aufgeführt, die logische Schnittstellen erfordern, z. B. „So konfigurieren Sie einen IPv6-über-IPv4-Tunnel“ auf Seite 205.

Zu den physikalischen Schnittstellen gehören Schnittstellen, die in das System integriert sind und separat erworbene Schnittstellen. Jede Schnittstelle befindet sich auf einer *Netzwerkschnittstellenkarte* (NIC).

Integrierte NICs sind bereits beim Kauf auf einem System vorhanden. Ein Beispiel einer Schnittstelle auf einer integrierten NIC ist die *primäre Netzwerkschnittstelle*, z. B. `eri0` oder `hme0`. Die primäre Netzwerkschnittstelle eines Systems muss bereits während der Installation konfiguriert werden.

NICs wie `eri` und `hme` verfügen über nur eine Schnittstelle. Es gibt jedoch auch zahlreiche NICs mit mehreren Schnittstellen. Eine NIC mit mehreren Schnittstellen wie `qfe` verfügt über vier Schnittstellen, `qfe0` – `qfe3`. Das Oracle Solaris-Installationsprogramm erkennt alle bei der Installation verfügbaren Schnittstellen und fragt, ob diese Schnittstellen konfiguriert werden sollen. Sie können diese Schnittstellen dann während des Bootens oder zu einem späteren Zeitpunkt konfigurieren.

Hinweis – NICs werden auch als *Netzwerkadapter* bezeichnet.

Zusätzlich zu den integrierten NICs können Sie separat erworbene NICs zu einem System hinzufügen. Sie bauen eine separat erworbene NIC gemäß den Anweisungen des Herstellers

ein. Dann müssen Sie die Schnittstellen auf der NIC konfigurieren, so dass sie für die Weitergabe von Daten verwendet werden können.

Im Folgenden sind Gründe aufgeführt, warum nach der Installation zusätzliche Schnittstellen auf einem System konfiguriert werden müssen:

- Sie möchten ein System so aufrüsten, dass es ein Multihomed-Host wird. Weitere Informationen zu Multihomed-Hosts finden Sie unter „Konfiguration von Multihomed-Hosts“ auf Seite 134.
- Sie möchten einen Host zu einem Router ändern. Anweisungen zur Konfiguration von Routern finden Sie unter „Konfiguration eines IPv4-Routers“ auf Seite 126.
- Sie möchten eine Schnittstelle zu einer IPMP-Gruppe hinzufügen. Informationen zu Schnittstellen in einer IPMP-Gruppe finden Sie unter „IPMP-Schnittstellenkonfigurationen“ auf Seite 787.

▼ So fügen Sie eine physikalische Schnittstelle nach der Installation hinzu (nur Solaris10 3/05)

Bevor Sie beginnen Legen Sie die IPv4-Adressen fest, die Sie für die zusätzlichen Schnittstellen verwenden möchten.

Die zu konfigurierende physikalische Schnittstelle muss bereits auf dem System vorhanden sein. Informationen zur Installation separat erworbener NIC-Hardware finden Sie in der Herstellerdokumentation, die mit der NIC ausgeliefert wurde.

Im folgenden Verfahren wird davon ausgegangen, dass Sie nach der Installation der neuen Schnittstelle einen Neustart zur Übernahme der Konfiguration vorgenommen haben.

Hinweis – Das folgende Verfahren gilt nur für Solaris 10 3/05. Wenn Sie ein Update von Oracle Solaris 10 verwenden, lesen Sie „So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation“ auf Seite 159.

---

1. **Nehmen Sie auf dem System mit den zu konfigurierenden Schnittstellen die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Konfigurieren und plumben Sie jede Schnittstelle.**

   ```
   # ifconfig interface plumb up
   ```

Für `qfe0` geben Sie z. B. Folgendes ein:

```
# ifconfig qfe0 plumb up
```

Hinweis – Schnittstellen, die explizit mit dem Befehl `ifconfig` konfiguriert wurden, behalten ihre Konfiguration nach einem Neustart nicht bei.

---

3. **Weisen Sie der Schnittstelle eine IPv4-Adresse und eine Netzmaske zu.**

   `# ifconfig` *interface IPv4-address* `netmask+`*netmask*

   Für `qfe0` geben Sie z. B. Folgendes ein:

   ```
   # ifconfig qfe0 10.0.0.32 netmask + 255.255.255.0
   ```

4. **Prüfen Sie, ob die neu konfigurierten Schnittstellen geplumbt (aktiviert) konfiguriert wurden bzw. „`UP`“ sind.”**

   ```
   # ifconfig -a
   ```

   Prüfen Sie die Statuszeile jeder angezeigten Schnittstelle. Achten Sie darauf, dass die Ausgabe das Flag `UP` in der Statuszeile enthält, z. B.:

   ```
   qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
   ```

5. **(Optional) Sorgen Sie dafür, dass die Schnittstellenkonfiguration auch nach einem Neustart beibehalten wird. Führen Sie dazu die folgenden Schritte aus:**

   a. **Erstellen Sie für jede zu konfigurierende Schnittstelle eine `/etc/hostname.`*Schnittstelle*-Datei.**

      Zum Hinzufügen der Schnittstelle `qfe0` erstellen Sie z. B. die folgende Datei:

      ```
      # vi /etc/hostname.qfe0
      ```

   b. **Bearbeiten Sie die `/etc/hostname.`*Schnittstelle*-Datei.**

      Geben Sie mindestens die IPv4-Adresse der Schnittstelle in die Datei ein. Sie können auch einen Netzmaske oder andere Konfigurationsinformationen in die Datei eingeben.

      Hinweis – Wie Sie eine IPv6-Adresse für eine Schnittstelle hinzufügen, lesen Sie unter „Modifizieren einer IPv6-Schnittstellenkonfiguration für Hosts und Server“ auf Seite 196

      ---

   c. **Fügen Sie Einträge für die neuen Schnittstellen in die `/etc/inet/hosts`-Datei ein.**

   d. **Führen Sie einen Neustart durch, um die neue Konfiguration zu übernehmen.**

      ```
      # reboot -- -r
      ```

e. **Vergewissern Sie sich, dass die in der** `/etc/hostname.` *Schnittstelle*-**Datei erstellte Schnittstelle konfiguriert wurde.**

```
# ifconfig -a
```

Beispiel 5–10 Konfiguration einer Schnittstelle nach der Systeminstallation

Im folgenden Beispiel wird gezeigt, wie Sie zwei Schnittstellen, `qfe0` und `qfe1` hinzufügen. Diese Schnittstellen sind als primäre Netzwerkschnittstelle `hme0` an das gleiche Netzwerk angehängt. Diese Schnittstellenkonfiguration bleibt wirksam, bis Sie das System neu booten. Ein Beispiel, wie Sie dafür sorgen, dass eine Schnittstellenkonfiguration auch nach einem Neustart beibehalten wird, finden Sie in Beispiel 6–2. Der in diesem Beispiel verwendete Befehl `dladm` steht jedoch erst ab Solaris 10 1/06 zur Verfügung.

```
# ifconfig qfe0 plumb up
# ifconfig qfe1 plumb up
# ifconfig qfe0 10.0.0.32 netmask 255.0.0.0
# ifconfig qfe1 10.0.0.33 netmask 255.0.0.0

# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.14 netmask ff000000 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 10.0.0.32 netmask ff000000 broadcast 10.255.255.255
        ether 8:0:20:c8:f4:1d
qfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 4
        inet 10.0.0.33 netmask ff000000 broadcast 10.255.255.255
        ether 8:0:20:c8:f4:1e
```

Siehe auch

- Informationen zur Konfiguration einer IPv6-Adresse für eine Schnittstelle finden Sie unter „So aktivieren Sie eine IPv6-Schnittstelle für die aktuelle Sitzung“ auf Seite 186.
- Informationen zum Einrichten der Failover-Erkennung und Failback für Schnittstellen, die Network Multipathing (IPMP) verwenden, finden Sie in Kapitel 31, „Verwaltung von IPMP (Aufgaben)“.

▼ So entfernen Sie eine physikalische Schnittstelle (nur Solaris 10 3/05)

Hinweis – Das folgende Verfahren gilt nur für Solaris 10 3/05. Wenn Sie ein Update auf Oracle Solaris 10 verwenden, lesen Sie „So entfernen Sie eine physikalische Schnittstelle“ auf Seite 162.

---

1. **Nehmen Sie auf dem System mit den zu entfernenden Schnittstellen die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Entfernen Sie die physikalische Schnittstelle.**

   Geben Sie den folgenden `ifconfig`-Befehl ein:

   ```
   # ifconfig interfacedown unplumb
   ```

   Zum Entfernen der Schnittstelle `eri1` geben Sie z. B. Folgendes ein:

   ```
   # ifconfig eri1 down unplumb
   ```

Konfiguration von VLANs (nur Solaris 10 3/05)

Hinweis – Dieser Abschnitt enthält Informationen zur Konfiguration von VLANs für Benutzer von Solaris 10 3/05. Wenn Sie ein Update auf Oracle Solaris 10 verwenden, lesen Sie „Verwalten von virtuellen lokalen Netzwerken" auf Seite 167.

Virtuelle lokale Netzwerke (VLANs) werden häufig dazu verwendet, Gruppen von Netzwerkbenutzern in überschaubarer Broadcast-Domänen aufzuteilen, um eine logische Segmentierung von Arbeitsgruppen vorzunehmen oder um Sicherheitsrichtlinien in jedem logischen Segment durchzusetzen. Bei mehreren VLANs auf einem Adapter kann ein Server mit einem Adapter über mehrere logische IP-Teilnetze verfügen. Standardmäßig können 512 VLANs für jeden VLAN-konformen Adapter auf Ihrem Server definiert werden.

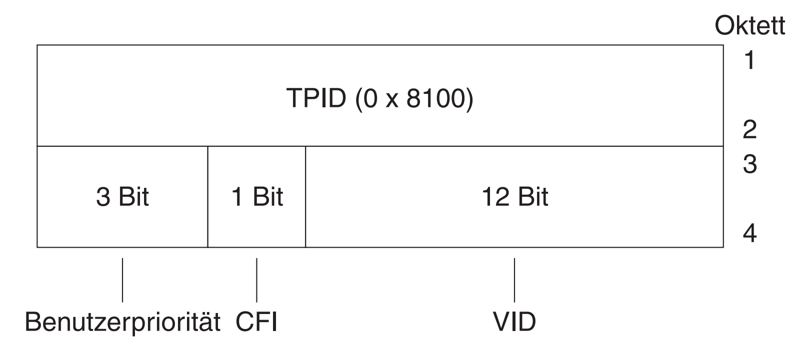
Falls Ihr Netzwerk keine Mehrfach-VLANs erfordert, können Sie die Standardkonfiguration verwenden und es ist keine erweiterte Konfiguration erforderlich.

Einen Überblick zu VLANs finden Sie unter „Einführung in die VLAN-Topologie" auf Seite 167.

VLANs können auf Grundlage verschiedener Kriterien erstellt werden, aber jedem VLAN muss ein VLAN-Tag oder eine VLAN-ID (VID) zugeordnet sein. Die VID ist ein 12-Bit-Bezeichner zwischen 1 und 4094, der ein VLAN eindeutig gekennzeichnet. Für jede Netzwerkschnittstelle (z. B. `ce0`, `ce1`, `ce2` usw.) können 512 mögliche VLANs erstellt werden. Da IP-Teilnetze weit verbreitet sind, verwenden Sie IP-Teilnetze beim Einrichten einer VLAN-Netzwerkschnittstelle. Dies bedeutet, dass jede VID, die einer VLAN-Schnittstelle einer physikalischen Netzwerkschnittstelle zugewiesen wird, zu verschiedenen Teilnetzen gehört.

Für das Tagging eines Ethernet-Frames muss ein Tag-Header zum Frame hinzugefügt werden. Der Header wird unmittelbar nach der MAC-Zieladresse und der MAC-Quelladresse eingefügt. Der Tag-Header besteht aus 2 Byte des Ethernet Tag Protocol Identifier (TPID, 0x8100) und 2 Byte der Tag Control Information (TCI). Das Ethernet Tag-Header-Format wird in der folgenden Abbildung gezeigt.

ABBILDUNG 5–4 Ethernet Tag-Header-Format



So werden statische VLANs konfiguriert (nur Solaris 10 3/05)

Hinweis – Dieses Verfahren enthält Informationen zur Konfiguration von VLANs für Benutzer von Solaris 10 3/05. Wenn Sie ein Update auf Oracle Solaris 10 verwenden, lesen Sie „So konfigurieren Sie ein VLAN“ auf Seite 171.

---

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Ermitteln Sie die auf Ihrem System verwendeten Schnittstellentypen.**

   Der Netzwerkadapter in Ihrem System wird eventuell nicht durch die Buchstaben ce gekennzeichnet, die für ein VLAN erforderlich sind.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4>
mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 2
        inet 129.156.200.77 netmask ffffff00 broadcast
129.156.200.255
```

3 Erstellen Sie für jedes VLAN, das für jeden Adapter auf dem Server konfiguriert wird, eine `hostname.ce`*Nummer*-Datei (`hostname6.ce`*Nummer*-Datei bei IPv6).

Verwenden Sie das folgende Benennungsformat, das sowohl die VID als auch den physikalischen Anschlusspunkt (Physical Point Of Attachment, PPA) enthält:

VLAN logischer PPA = 1000 * *VID* + *Geräte-PPA* `ce123000 = 1000*123 + 0`

Beispiel: `hostname.ce123000`

VLAN logischer PPA = 1000 * *VID* + *Geräte-PPA* `ce11000 = 1000*11 + 0`

Beispiel: `hostname.ce11000`

Dieses Format schränkt die maximale Anzahl der zu konfigurierenden PPAs (Instanzen) in der `/etc/path_to_inst`-Datei auf 1000 ein.

Angenommen, auf einem Server hat der Sun Gigabit Ethernet/P 3.0-Adapter die Instanz 0, die zu zwei VLANs mit den VIDs 123 und 224 gehört. In diesem Fall verwenden Sie `ce123000` bzw. `ce224000` für die zwei VLAN PPAs.

4 Konfigurieren eines virtuellen VLAN- Geräts:

Sie können die folgenden Beispiele von `ifconfig` verwenden:

```
# ifconfig ce123000 plumb up
# ifconfig ce224000 plumb up
```

Die Ausgabe von `ifconfig -a` auf einem System den mit VLAN-Geräten `ce123000` und `ce224000` sollte Folgendem ähneln:

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 129.144.131.91 netmask ffffff00 broadcast 129.144.131.255
        ether 8:0:20:a4:4f:b8
ce123000: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 199.199.123.3 netmask ffffff00 broadcast 199.199.123.255
        ether 8:0:20:a4:4f:b8
ce224000: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 4
        inet 199.199.224.3 netmask ffffff00 broadcast 199.199.224.255
        ether 8:0:20:a4:4f:b8
```

5 Richten Sie das VLAN-Tagging und die VLAN-Ports auf dem Switch so ein, dass sie sich mit den VLANs decken, die Sie auf dem Server eingerichtet haben.

Bei den Beispielen in Schritt 4 richten Sie die VLAN-Ports 123 und 224 auf dem Switch oder die VLAN-Ports 10 und 11 ein.

Weitere Informationen zum Einrichten des VLAN-Taggings und der Ports entnehmen Sie bitte der Dokumentation, die mit Ihrem Switch ausgeliefert wurde.

KAPITEL 6

Verwalten von Netzwerkschnittstellen (Aufgaben)

Dieses Kapitel enthält Aufgaben und Informationen zu Netzwerkschnittstellen:

- „Schnittstellenverwaltung (Übersicht der Schritte)" auf Seite 156
- „Grundlagen zur Verwaltung physikalischer Schnittstellen" auf Seite 165
- „Grundlagen zur Verwaltung physikalischer Schnittstellen" auf Seite 157

Neuerungen bei der Verwaltung von Netzwerkschnittstellen

Die Informationen in diesem Kapitel beschreiben die Schnittstellenkonfiguration ab dem Solaris-Release 10 1/06. Wenn Sie das ursprüngliche Release von Solaris 10 (3/05) verwenden, lesen Sie bitte „Verwalten der Schnittstellen in Solaris 10 3/05" auf Seite 147. Eine vollständige Liste der neuen Oracle Solaris-Funktionen und eine Beschreibung der Oracle Solaris-Versionen finden Sie im Handbuch *Neuerungen in Oracle Solaris 9 10/10*.

Unter Solaris 10 1/06 wurden die folgenden neuen Funktionen eingeführt:

- Der neue Befehl `dladm` zum Anzeigen des Schnittstellenstatus wird unter „So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation" auf Seite 159 beschrieben.
- Die VLAN-Unterstützung wurde auf GLDv3-Schnittstellen erweitert, wie unter „Verwalten von virtuellen lokalen Netzwerken" auf Seite 167 beschrieben.
- Die Unterstützung von Linkaggregationen wird unter „Übersicht der Link-Aggregationen" auf Seite 173 beschrieben.

Unter Solaris 10 7/07 wird die Datei `/etc/inet/ipnodes` nicht mehr benötigt. Sie verwenden `/etc/inet/ipnodes` nur für frühere Solaris 10-Releases, wie es in den jeweiligen Verfahren beschrieben wird.

Schnittstellenverwaltung (Übersicht der Schritte)

In der folgenden Tabelle werden verschiedene Aufgaben zum Konfigurieren von Netzwerkschnittstellen aufgeführt, darunter spezielle Konfigurationen wie VLANs und Linkaggregationen. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen Aufgaben sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
Prüfen des Status der Schnittstellen eines Systems.	Listen Sie alle Schnittstellen in einem System auf, und prüfen Sie, welche Schnittstellen bereits installiert und geplumbt (aktiviert) wurden.	„So beziehen Sie den Schnittstellenstatus“ auf Seite 157
Hinzufügen einer einzelnen Schnittstelle nach der Systeminstallation.	Ändern Sie ein System zu einem Multihomed-Host oder -Router, indem Sie eine weitere Schnittstelle konfigurieren.	„So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation“ auf Seite 159
SPARC: Sicherstellen der Einmaligkeit der MAC-Adresse der Schnittstelle.	Stellen Sie sicher, dass die Schnittstelle mit der werkseitigen MAC-Adresse konfiguriert ist, und nicht mit der MAC-Adresse des Systems (nur SPARC).	„SPARC: So stellen Sie sicher, dass die MAC-Adresse einer Schnittstelle einmalig ist“ auf Seite 163
Planen eines virtuellen lokalen Netzwerks (VLAN).	Führen Sie die erforderlichen Planungsaufgaben vor dem Erstellen eines VLAN aus.	„So planen Sie eine VLAN-Konfiguration“ auf Seite 170
Konfiguration eines VLAN.	Erstellen und modifizieren Sie VLANs in Ihrem Netzwerk.	„So konfigurieren Sie ein VLAN“ auf Seite 171
Planung für Aggregationen.	Planen Sie die Aggregation und führen Sie die erforderlichen Planungsaufgaben aus, bevor Sie Aggregationen konfigurieren.	„Übersicht der Link-Aggregationen“ auf Seite 173
Konfiguration einer Aggregation.	Führen Sie die erforderlichen Aufgaben aus, um Aggregationen zu verknüpfen.	„So erstellen Sie eine Linkaggregation“ auf Seite 177
Planen für und Konfiguration einer IPMP-Gruppe.	Konfigurieren Sie Failover und Failback für Schnittstellen, die Mitglieder einer IPMP-Gruppe sind.	„So planen Sie für eine IPMP-Gruppe“ auf Seite 799 „So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen“ auf Seite 801

Grundlagen zur Verwaltung physikalischer Schnittstellen

Nach der Oracle Solaris-Installation kann es aus den folgenden Gründen erforderlich werden, Schnittstellen auf einem System zu konfigurieren oder zu verwalten:

- Sie möchten ein System so aufrüsten, dass es ein Multihomed-Host wird. Weitere Informationen hierzu finden Sie unter „Konfiguration von Multihomed-Hosts“ auf Seite 134.
- Sie möchten einen Host zu einem Router ändern. Anweisungen zur Konfiguration von Routern finden Sie unter „Konfiguration eines IPv4-Routers“ auf Seite 126.
- Sie möchten Schnittstellen als Teil eines VLAN konfigurieren. Weitere Informationen hierzu finden Sie unter „Verwalten von virtuellen lokalen Netzwerken“ auf Seite 167.
- Sie möchten Schnittstellen als Mitglieder einer Aggregation konfigurieren. Weitere Informationen hierzu finden Sie unter „Übersicht der Link-Aggregationen“ auf Seite 173.
- Sie möchten eine Schnittstelle zu einer IPMP-Gruppe hinzufügen. Anweisungen zur Konfiguration einer IPMP-Gruppe finden Sie unter „Konfiguration von IPMP-Gruppen“ auf Seite 799

Dieser Abschnitt enthält Informationen zur Konfiguration einzelner Netzwerkschnittstellen; ab Solaris 10 1/06. Informationen zur Konfiguration von Schnittstellen, die in eine der folgenden Gruppen fallen, finden Sie in den folgenden Abschnitten:

- Informationen zur Konfiguration von Schnittstellen in einem VLAN finden Sie unter „Verwalten von virtuellen lokalen Netzwerken“ auf Seite 167.
- Informationen zur Konfiguration von Schnittstellen in einer Aggregation finden Sie unter „Übersicht der Link-Aggregationen“ auf Seite 173.
- Informationen zur Konfiguration von Schnittstellen als Mitglieder von IPMP-Gruppen finden Sie unter „Konfiguration von IPMP-Gruppen“ auf Seite 799.

▼ So beziehen Sie den Schnittstellenstatus

Ab Solaris 10 1/06: Mit diesem Verfahren wird festgestellt, welche Schnittstellen aktuell auf einem System verfügbar sind und welchen Status sie aufweisen. Dieses Verfahren zeigt auch an, welche Schnittstellen aktuell geplumbt (aktiviert) sind. Wenn Sie eine frühere Version als Solaris 10 3/05 verwenden, lesen Sie „So zeigen Sie Informationen zu einer bestimmten Schnittstelle an“ auf Seite 221.

1 **Nehmen Sie auf dem System mit den zu konfigurierenden Schnittstellen die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Stellen Sie fest, welche Schnittstellen derzeit auf dem System installiert sind.

```
# dladm show-link
```

In diesem Schritt wird der `dladm`-Befehl verwendet, der in der Manpage `dladm`(1M) ausführlich beschrieben wird. Dieser Befehl meldet alle gefundenen Schnittstellentreiber, unabhängig davon, ob die Schnittstellen bereits konfiguriert wurden.

3 Stellen Sie fest, welche Schnittstellen auf dem System derzeit geplumbt (aktiviert) sind.

```
# ifconfig -a
```

Der Befehl `ifconfig` bietet zahlreiche zusätzliche Funktionen, einschließlich dem Plumben (Aktivieren) einer Schnittstelle. Weitere Informationen finden Sie in der Manpage `ifconfig`(1M).

Beispiel 6–1 Beziehen des Status einer Schnittstelle mit dem `dladm`-Befehl

Im folgenden Beispiel wird die Statusanzeige des `dladm`-Befehls gezeigt.

```
# dladm show-link
ce0             type: legacy    mtu: 1500       device: ce0
ce1             type: legacy    mtu: 1500       device: ce1
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1
bge2            type: non-vlan  mtu: 1500       device: bge2
```

Die Ausgabe des Befehls `dladm show-link` zeigt, dass vier Schnittstellentreiber auf dem lokalen Host verfügbar sind. Die Schnittstellen `ce` und `bge` können für VLANs konfiguriert werden. Jedoch können nur die GLDV3-Schnittstellen des Typs `nicht-VLAN` für Linkaggregationen verwendet werden.

Im folgenden Beispiel wird die Statusanzeige des Befehls `ifconfig -a` gezeigt.

```
# ifconfig -a
 lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu
8232 index 1
         inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 3
         inet 192.168.84.253 netmask ffffff00 broadcast 192.168.84.255
        ether 0:3:ba:7:84:5e
bge0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,DHCP,IPv4>mtu 1500 index 2
         inet 10.8.57.39 netmask ffffff00 broadcast 10.8.57.255
        ether 0:3:ba:29:fc:cc
```

Die Ausgabe des Befehls `ifconfig -a` zeigt die Statistiken nur für zwei Schnittstellen an: `ce0` und `bge0`. Dieser Ausgabe zeigt, dass nur `ce0` und `bge0` geplumbt (aktiviert) wurden und für die Übertragung von Netzwerkverkehr bereit sind. Diese Schnittstellen können in einem VLAN verwendet werden. Da `bge0` geplumbt (aktiviert) wurde, können Sie diese Schnittstelle nicht mehr in einer Aggregation verwenden.

▼ So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation

Mit dem folgenden Verfahren werden Schnittstellen konfiguriert. Wenn Sie Solaris 10 3/05 einsetzen, führen Sie das Verfahren „So fügen Sie eine physikalische Schnittstelle nach der Installation hinzu (nur Solaris10 3/05)“ auf Seite 149 aus.

Bevor Sie beginnen

- Legen Sie die IPv4-Adressen fest, die Sie für die zusätzlichen Schnittstellen verwenden möchten.
- Stellen Sie sicher, dass die zu konfigurierende physikalische Schnittstelle im System installiert ist. Informationen zur Installation von separat erworbener NIC-Hardware finden Sie in der Herstellerdokumentation, die mit der NIC ausgeliefert wurde.
- Wenn Sie die Schnittstelle gerade installiert haben, führen Sie einen Neustart zur Übernahme der neuen Konfiguration durch, bevor Sie mit der nächsten Aufgabe beginnen.

1. **Nehmen Sie auf dem System mit den zu konfigurierenden Schnittstellen die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Stellen Sie fest, welche Schnittstellen derzeit auf dem System installiert sind.**

   ```
   # dladm show-link
   ```

3. **Konfigurieren und plumben Sie jede Schnittstelle.**

   `# ifconfig` *interface* `plumb up`

   Für `qfe0` geben Sie z. B. Folgendes ein:

   ```
   # ifconfig qfe0 plumb up
   ```

   Hinweis – Schnittstellen, die explizit mit dem Befehl `ifconfig` konfiguriert wurden, behalten ihre Konfiguration nach einem Neustart nicht bei.

   ---

4. **Weisen Sie der Schnittstelle eine IPv4-Adresse und eine Netzmaske zu.**

   `# ifconfig` *interface IPv4-address* `netmask+`*netmask*

   Für `qfe0` geben Sie z. B. Folgendes ein:

   ```
   # ifconfig
   qfe0 192.168.84.3 netmask + 255.255.255.0
   ```

Hinweis – Sie können eine IPv4-Adresse entweder in der traditionellen IPv4-Notation oder in der CIDR-Notation angeben.

---

5. **Prüfen Sie, ob die neu konfigurierten Schnittstellen geplumbt (aktiviert) konfiguriert wurden bzw. „`UP`“ sind.“**

```
# ifconfig
-a
```

Prüfen Sie die Statuszeile jeder angezeigten Schnittstelle. Achten Sie darauf, dass die Ausgabe das Flag `UP` in der Statuszeile enthält, z. B.:

```
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 2
```

6. **(Optional) Sorgen Sie dafür, dass die Schnittstellenkonfiguration auch nach einem Neustart beibehalten wird. Führen Sie dazu die folgenden Schritte aus:**

   a. **Erstellen Sie für jede zu konfigurierende Schnittstelle eine `/etc/hostname.`*Schnittstelle*-Datei.**

   Zum Hinzufügen der Schnittstelle `qfe0` erstellen Sie z. B. die folgende Datei:

   ```
   # vi /etc/hostname.qfe0
   ```

   Hinweis – Wenn Sie alternative Hostname-Dateien für die gleiche Schnittstelle erstellen, müssen die alternativen Dateien ebenfalls dem Benennungsformat`hostname folgen.[0–9]*`, wie z. B. `hostname.qfe0.a123`. Namen wie`hostname.qfe0.bak` oder `hostname.qfe0.old` sind ungültig und werden von Skripten beim Booten des Systems ignoriert.

   Beachten Sie außerdem, dass eine angegebene Schnittstelle nur eine entsprechende Hostname-Datei haben darf. Wenn Sie eine alternative Hostname-Datei für eine Schnittstelle mit einem gültigen Dateinamen angeben, wie beispielsweise `/etc/hostname.qfe` und `/etc/hostname.qfe.a123` , versuchen die Boot-Skripten, die Konfiguration durchzuführen, indem sie die Inhalte beider Hostname-Dateien referenzieren, woraus Fehler resultieren würden. Um diese Fehler zu vermeiden, geben Sie einen ungültigen Dateinamen für die Hostname-Datei an, die Sie in einer bestimmten Konfiguration nicht verwenden möchten.

   ---

   b. **Bearbeiten Sie die `/etc/hostname.`*Schnittstelle*-Datei.**

   Geben Sie mindestens die IPv4-Adresse der Schnittstelle in die Datei ein. Sie können die traditionelle IPv4-Notation oder die CIDR-Notation verwenden, um die IP-Adresse der Schnittstelle anzugeben. Sie können auch einen Netzmaske oder andere Konfigurationsinformationen in die Datei eingeben.

Hinweis – Wie Sie eine IPv6-Adresse für eine Schnittstelle hinzufügen, lesen Sie unter „Modifizieren einer IPv6-Schnittstellenkonfiguration für Hosts und Server“ auf Seite 196

---

c. **Für Solaris 10 11/06 und frühere Versionen von Oracle Solaris 10 fügen Sie die Einträge für die neue Schnittstelle in die `/etc/inet/ipnodes`-Datei ein.**

d. **Fügen Sie Einträge für die neuen Schnittstellen in die `/etc/inet/hosts`-Datei ein.**

e. **Führen Sie einen Neustart durch, um die neue Konfiguration zu übernehmen.**

```
# reboot -- -r
```

f. **Vergewisseren Sie sich, dass die in der `/etc/hostname.` *Schnittstelle*-Datei erstellte Schnittstelle konfiguriert wurde.**

```
# ifconfig -a
```

Beispiele finden Sie unter Beispiel 6–2.

Beispiel 6–2 Hinzufügen von persistenten Schnittstellenkonfiguration

Im folgenden Beispiel wird gezeigt, wie Sie die Schnittstellen `qfe0` und `qfe1` für einen Host konfigurieren. Die Konfiguration dieser Schnittstellen wird auch nach einem Neustart beibehalten.

```
# dladm show-link
eri0    type: legacy    mtu: 1500       device: eri0
qfe0    type: legacy    mtu: 1500       device: qfe0
qfe1    type: legacy    mtu: 1500       device: qfe1
qfe2    type: legacy    mtu: 1500       device: qfe2
qfe3    type: legacy    mtu: 1500       device: qfe3
bge0    type: non-vlan  mtu: 1500       device: bge0
# vi /etc/hostname.qfe0
192.168.84.3 netmask 255.255.255.0
# vi /etc/hostname.qfe1
192.168.84.72 netmask 255.255.255.0
# vi /etc/inet/hosts
# Internet host table
#
127.0.0.1       localhost
10.0.0.14       myhost
192.168.84.3       interface-2
192.168.84.72       interface-3
For Solaris 10 11/06 and earlier releases:# vi /etc/inet/ipnodes
10.0.0.14 myhost
192.168.84.3       interface-2
192.168.84.72       interface-3
```

An diesem Punkt starten Sie das System neu, um die neue Konfiguration zu übernehmen.

```
# reboot -- -r
```

Nachdem das System neu gestartet wurde, überprüfen Sie die Schnittstellenkonfiguration.

```
ifconfig -a
# ifconfig -a lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu
8232 index 1
         inet 127.0.0.1 netmask ff000000
eri0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         inet 10.0.0.14netmask ff000000 broadcast 10.255.255.255
         ether 8:0:20:c1:8b:c3
qfe0:flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
      inet 192.168.84.3 netmask ffffff00 broadcast 192.255.255.255
      ether 8:0:20:c8:f4:1d
qfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 4
         inet 192.168.84.72 netmask ffffff00 broadcast 10.255.255.255
        ether 8:0:20:c8:f4:1e
```

Siehe auch

- Informationen zur Konfiguration einer IPv6-Adresse für eine Schnittstelle finden Sie unter „So aktivieren Sie eine IPv6-Schnittstelle für die aktuelle Sitzung“ auf Seite 186.
- Informationen zum Einrichten von Failover-Erkennung und Failback für Schnittstellen, die Network Multipathing (IPMP) verwenden, finden Sie in Kapitel 31, „Verwaltung von IPMP (Aufgaben)“.

▼ So entfernen Sie eine physikalische Schnittstelle

Mit dem folgenden Verfahren entfernen Sie eine physikalische Schnittstelle. Wenn Sie Solaris 10 3/05 verwenden, lesen Sie „So entfernen Sie eine physikalische Schnittstelle (nur Solaris 10 3/05)“ auf Seite 151.

1. **Nehmen Sie auf dem System mit den zu entfernenden Schnittstellen die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Entfernen Sie die physikalische Schnittstelle.**

   \# **ifconfig** *interface* **down unplumb**

   Zum Entfernen der Schnittstelle `qfe1` geben Sie z. B. Folgendes ein:

   ```
   # ifconfig qfe1 down unplumb
   ```

▼ SPARC: So stellen Sie sicher, dass die MAC-Adresse einer Schnittstelle einmalig ist

Mit dem folgenden Verfahren konfigurieren Sie MAC-Adressen.

Einige Anwendungen erfordern, dass jede Schnittstelle auf einem Host über eine einmalige MAC-Adresse verfügt. Jedoch hat jedes SPARC-basierte System eine systemweit geltende MAC-Adresse, die standardmäßig von allen Schnittstellen verwendet wird. Im Folgenden sind zwei Situationen aufgeführt,bei denen Sie die werkseitigen MAC-Adressen für die Schnittstellen auf einem SPARC-System konfigurieren möchten.

- Bei Linkaggregationen sollten Sie die werkseitigen MAC-Adressen der Schnittstellen in der Aggregation-Konfiguration verwenden.
- Bei IPMP-Gruppen muss jede Schnittstelle in der Gruppe über eine einmalige MAC-Adresse verfügen. Diese Schnittstellen müssen die werkseitigen MAC-Adressen verwenden.

Der EEPROM-Parameter `local-mac-address?` gibt an, ob alle Schnittstellen eines SPARC-Systems die systemweite MAC-Adresse oder die einmaligen MAC-Adressen verwenden. Im nächsten Verfahren wird gezeigt, wie Sie den `eeprom`-Befehl verwenden, um den aktuellen Wert des `local-mac-address?`-Parameters zu prüfen und gegebenenfalls zu ändern.

1 **Nehmen Sie auf dem System mit den zu konfigurierenden Schnittstellen die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Stellen Sie fest, ob alle Schnittstellen im System derzeit die systemweite MAC-Adresse verwenden.**

```
# eeprom local-mac-address?
local-mac-address?=false
```

In diesem Beispiel deutet die Antwort auf den `eeprom`-Befehl, `local-mac-address?=false`, darauf hin, dass alle Schnittstellen die systemweite MAC-Adresse verwenden. Der Wert `local-mac-address?=false` muss zu `local-mac-address?=true` geändert werden, bevor die Schnittstellen der Mitglieder einer IPMP-Gruppe werden können. Sie sollten `local-mac-address?=false` auch für Aggregationen zu `local-mac-address?=true` ändern.

3 **Gegebenenfalls ändern Sie den Wert von `local-mac-address?` wie folgt:**

```
# eeprom local-mac-address?=true
```

Wenn Sie das System neu starten, verwenden die Schnittstellen mit dem werkseitigen MAC-Adressen jetzt diese werkseitigen Einstellungen statt der systemweiten MAC-Adresse. Schnittstellen ohne werkseitige MAC-Adresse verwenden weiterhin die systemweite MAC-Adresse.

4 **Prüfen Sie die MAC-Adressen aller Schnittstellen des Systems.**

Suchen Sie nach Fällen, bei denen mehrere Schnittstellen die gleiche MAC-Adresse aufweisen. In diesem Beispiel verwenden alle Schnittstellen die systemweite MAC-Adresse `8:0:20:0:0:1` .

```
ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
      inet 127.0.0.1 netmask ff000000
hme0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 10.0.0.112 netmask ffffff80 broadcast 10.0.0.127
      ether 8:0:20:0:0:1
ce0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 10.0.0.114 netmask ffffff80 broadcast 10.0.0.127
      ether 8:0:20:0:0:1
ce1: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 10.0.0.118 netmask ffffff80 broadcast 10.0.0.127
      ether 8:0:20:0:0:1
```

Hinweis – Setzen Sie mit dem nächsten Schritt fort, wenn noch immer mehrere Schnittstellen die gleiche MAC-Adresse aufweisen. Andernfalls gehen Sie zum letzten Schritt.

---

5 **Falls erforderlich, konfigurieren Sie die verbleibenden Schnittstellen manuell, so dass alle Schnittstellen eine einmalige MAC-Adresse aufweisen.**

Geben Sie eine einmalige MAC-Adresse in die `/etc/hostname.`*Schnittstelle*-Datei für die entsprechende Schnittstelle ein.

Bei dem Beispiel in Schritt 4 konfigurieren Sie `ce0` und `ce1` mit lokal verwalteten MAC-Adressen. Um `ce1` mit der lokal verwalteten MAC-Adresse `06:05:04:03:02` zu konfigurieren, fügen Sie die folgende Zeile zur `/etc/hostname.ce1`-Datei hinzu:

```
ether 06:05:04:03:02
```

Hinweis – Um zu verhindern, dass manuell konfigurierte MAC-Adressen zu einem Konflikt mit anderen MAC-Adressen in Ihrem Netzwerk führen, müssen Sie stets *lokal verwaltete* MAC-Adressen gemäß der Definition in IEEE 802.3 konfigurieren.

Sie können auch den Befehl `ifconfig ether` verwenden, um die MAC-Adresse einer Schnittstelle für die aktuelle Sitzung zu konfigurieren. Mit `ifconfig` vorgenommene Änderungen werden jedoch nach einem Neustart nicht beibehalten. Einzelheiten finden Sie in der Manpage `ifconfig`(1M).

6 **Starten Sie das System neu.**

Grundlagen zur Verwaltung physikalischer Schnittstellen

Netzwerkschnittstellen stellen die Verbindung zwischen einem System und einem Netzwerk her. Ein Oracle Solaris-basiertes System kann über zwei Arten von Schnittstellen verfügen: physikalisch und logisch. *Physikalische Schnittstellen* bestehen aus einem Softwaretreiber und einem Anschluss, über den sie eine Verbindung mit dem Netzwerkmedium, z. B. ein Ethernet-Kabel, herstellen. Physikalische Schnittstellen können aus administrativen oder Verfügbarkeitsgründen gruppiert werden. *Logische Schnittstellen* werden in existierenden physikalischen Schnittstellen konfiguriert, in der Regel zum Hinzufügen von Adressen und zum Erzeugen von Tunnelendpunkten an den physikalischen Schnittstellen.

Hinweis – Logische Netzwerkschnittstellen werden in den Aufgaben beschrieben, in denen sie verwendet werden: IPv6-Aufgaben, IPMP-Aufgaben, DHCP-Aufgaben und andere.

Die meisten Computersysteme verfügen über mindestens eine physikalische Schnittstelle, die vom Hersteller in die Hauptplatine *integriert* wurde. Einige Systeme verfügen auch über mehrere integrierte Schnittstellen.

Neben den integrierten Schnittstellen können Sie einem System separat erworbene Schnittstellen hinzufügen. Eine separat erworbene Schnittstelle wird als *Netzwerkschnittstellenkarte* (NIC) bezeichnet. Eine NIC muss gemäß den Anweisungen des Herstellers in ein System eingebaut werden.

Hinweis – NICs werden auch als *Netzwerkadapter* bezeichnet.

Während der Systeminstallation erkennt das Oracle Solaris-Installationsprogramm alle physikalisch installierten Schnittstellen und zeigt deren Namen an. Mindestens eine Schnittstelle aus der Liste der Schnittstellen muss konfiguriert werden. Die erste von Ihnen während der Installation konfigurierte Schnittstelle wird zur *primären Netzwerkschnittstelle*. Die IP-Adresse der primären Netzwerkschnittstelle wird dem konfigurierten Hostnamen des Systems zugewiesen, der in der `/etc/nodename`-Datei gespeichert ist. Weitere Schnittstellen können Sie während der Installation oder zu einem späteren Zeitpunkt konfigurieren.

Netzwerkschnittstellennamen

Jede physikalische Schnittstelle wird durch einen eindeutigen Gerätenamen gekennzeichnet. Gerätenamen weisen die folgende Syntax auf:

```
<driver-name><instance-number>
```

Treibernamen auf Oracle Solaris-Systemen können `ce`, `hme`, `bge`, `e1000g` und verschiedene andere Gerätenamen enthalten. Die Variable *Instanznummer* kann einen Wert von Null bis *n* annehmen, abhängig davon, wie viele Schnittstellen mit diesem Treibertyp auf dem System installiert sind.

Betrachten Sie z. B. eine 100BASE-TX Fast Ethernet-Schnittstelle, die häufig als primäre Netzwerkschnittstelle auf Host- und Serversystemen eingesetzt wird. Einige typische Treibernamen für diese Schnittstelle sind `eri`, `qfe` und `hme`. Wenn sie als primäre Netzwerkschnittstelle verwendet wird, hat die Fast Ethernet-Schnittstelle einen Gerätenamen wie `eri0` oder `qfe0`.

NICs wie `eri` und `hme` verfügen über nur eine Schnittstelle. Es gibt jedoch auch zahlreiche NICs mit mehreren Schnittstellen. So verfügt die Quad Fast Ethernet-Karte (`qfe`) beispielsweise über vier Schnittstellen `qfe0` bis `qfe3`.

Plumben (aktivieren) einer Schnittstelle

Eine Schnittstelle muss *geplumbt* (aktiviert) werden, erst dann kann sie Datenverkehr zwischen dem System und dem Netzwerk übertragen. Der Plumbing-Prozess umfasst das Zuweisen eines Gerätenamens zu einer Schnittstelle. Dann werden die Datenströme so eingerichtet, dass die Schnittstelle vom IP-Protokoll verwendet werden kann. Sowohl physikalische Schnittstellen als auch logische Schnittstellen müssen mit geplumbt (aktiviert) werden. Schnittstellen werden entweder während der Bootsequenz oder explizit mit der entsprechenden Syntax des Befehls `ifconfig` geplumbt.

Wenn Sie eine Schnittstelle während der Installation konfigurieren, wird sie automatisch geplumbt. Wenn Sie sich während der Installation entschließen, keine zusätzlichen Schnittstellen auf dem System zu konfigurieren, so werden diese Schnittstellen nicht geplumbt.

Oracle Solaris-Schnittstellentypen

Ab Solaris 10 1/06 unterstützt Oracle Solaris die beiden folgenden Schnittstellentypen:

- **Legacy-Schnittstellen** – Hierzu gehören DLPI-Schnittstellen und GLDv2-Schnittstellen. Einige Legacy-Schnittstellentypen sind `eri`, `qfe` und `ce`. Bei der Prüfung des Schnittstellenstatus mit dem Befehl `dladm show-link` werden diese Schnittstellen als „Legacy“ aufgeführt.
- **Nicht-VLAN-Schnittstellen** – Hierbei handelt es sich um GLDv3-Schnittstellen.

Hinweis – Derzeit wird GLDv3 auf den folgenden Schnittstellentypen unterstützt: `bge`, `xge` und `e1000g`.

Verwalten von virtuellen lokalen Netzwerken

Hinweis – Wenn Sie Solaris 10 3/05 verwenden, lesen Sie „Konfiguration von VLANs (nur Solaris 10 3/05)“ auf Seite 152.

Ein *virtuelles lokales Netzwerk (VLAN)* ist eine Unterteilung eines lokalen Netzwerks auf der Sicherungsschicht des TCP/IP-Protokollstapels. Sie können VLANs für lokale Netzwerke erstellen, in denen die Switch-Technologie verwendet wird. Durch Zuweisen von Benutzergruppen zu VLANs können Sie die Netzwerkverwaltung verbessern und die Sicherheit für das gesamte lokale Netzwerk erhöhen. Außerdem können Sie Schnittstellen auf dem gleichen System verschiedenen VLANs zuordnen.

Eine Unterteilung Ihres lokalen Netzwerks in VLANs bietet sich an, wenn Sie folgende Bedingungen erfüllen müssen:

- Erstellen einer logischen Arbeitsgruppeneinteilung.

  Angenommen, alle Hosts auf einem Stockwerk eines Gebäudes sind mit einem Switch-basierten lokalen Netzwerk verbunden. In diesem Fall können Sie separate VLAN für jede Arbeitsgruppe auf diesem Stockwerk erstellen.
- Erzwingen unterschiedlicher Sicherheitsrichtlinien für die Arbeitsgruppen.

  Beispielsweise sind die Sicherheitsanforderungen der Finanzabteilung und der IT-Abteilung vollkommen unterschiedlich. Wenn beide Abteilungen das gleiche lokale Netzwerk nutzen, können Sie ein separates VLAN für jede Abteilung erstellen. Dann können Sie die erforderlichen Sicherheitsrichtlinien für jedes VLAN durchsetzen.
- Aufteilen der Arbeitsgruppen in überschaubare Broadcast-Domänen.

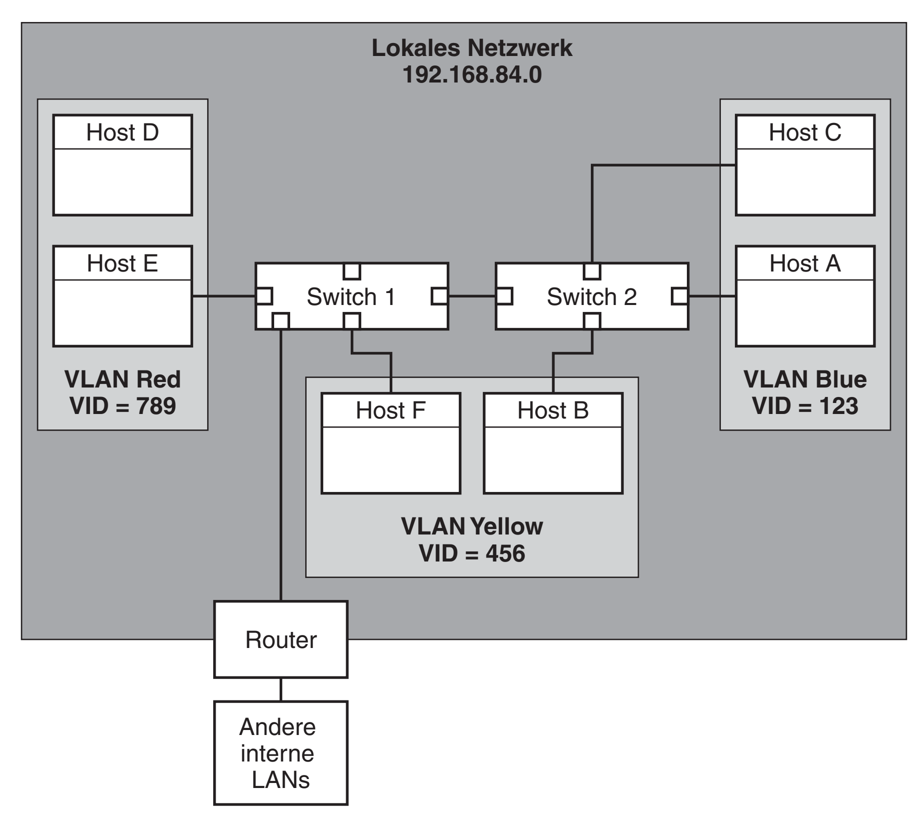
  Durch Verwenden von VLANs wird die Größe der Broadcast-Domänen verringert und die Netzwerkeffizienz erhöht.

Einführung in die VLAN-Topologie

Die LAN-Technologie mit Switches ermöglicht es Ihnen, Systeme in einem lokalen Netzwerk in VLANs zu strukturieren. Bevor Sie ein lokales Netzwerk in VLANs unterteilen, müssen Sie Switches einsetzen, die die VLAN-Technologie unterstützen. Sie können alle Ports auf einem Switch so konfigurieren, dass sie abhängig von der VLAN-Topologie nur ein VLAN oder mehrere VLANs versorgen. Jeder Switch-Hersteller unterstützt verschiedene Verfahren zur Konfiguration der Ports eines Switches.

Die folgende Abbildung zeigt ein lokales Netzwerk mit der Teilnetzadresse `192.168.84.0`. Dieses LAN ist in die drei VLANs Red, Yellow und Blue unterteilt.

ABBILDUNG 6–1 Lokales Netzwerk mit drei VLANs



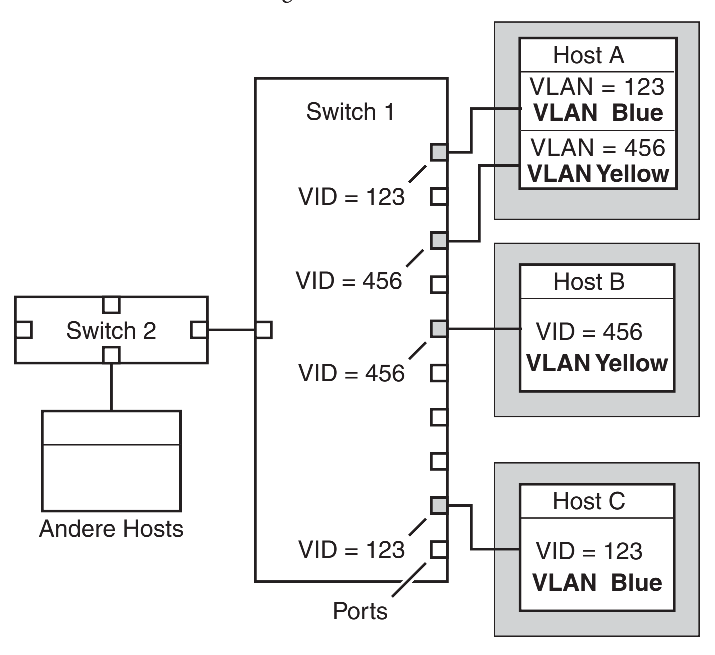
Die Konnektivität von LAN `192.168.84.0` ist Aufgabe der Switches 1 und 2. Das VLAN Red enthält die Systeme der Arbeitsgruppe „Accounting“. Die Systeme der Arbeitsgruppe „Human Resources“ sind dem VLAN Yellow zugewiesen. Die Systeme der Arbeitsgruppe „Information Technologies“ sind dem VLAN Blue zugewiesen.

VLAN-Tags und physikalischer Anschlusspunkt

Jedes VLAN in einem lokalen Netzwerk ist durch ein VLAN-Tag, oder eine *VLAN ID (VID)* gekennzeichnet. Die VID wird während der VLAN-Konfiguration zugewiesen. Die VID ist ein 12-Bit-Bezeichner zwischen 1 und 4094, der ein VLAN eindeutig kennzeichnet. In Abbildung 6–1 hat das VLAN Red die VID 789, das VLAN Yellow die VID 456 und das VLAN Blau die VID 123.

Wenn Sie Switches zur Unterstützung von VLANs konfigurieren, müssen Sie jedem Port eine VID zuweisen. Die VID des Ports muss der VID entsprechen, die der Schnittstelle zugewiesen wurde, die mit diesem Port verbunden ist. Dies wird in der folgenden Abbildung verdeutlicht.

ABBILDUNG 6–2 Switch-Konfiguration eines Netzwerks mit VLANs



In Abbildung 6–2 sind mehrere an unterschiedliche VLANs angeschlossene Hosts dargestellt. Zwei Hosts gehören dem gleichen VLAN an. In dieser Abbildung sind die primären Netzwerkschnittstellen der drei Hosts mit Switch 1 verbunden. Host A gehört zum VLAN Blue. Deswegen ist die Schnittstelle von Host A mit der·VID 123 konfiguriert. Diese Schnittstelle ist an Port 1 von Switch 1 angeschlossen, der dann mit der VID 123 konfiguriert wird. Host B gehört zum VLAN Yellow mit der VID 456. Die Schnittstelle von Host B ist an Port 5 von Switch 1 angeschlossen, der dann mit der VID 456 konfiguriert wird. Die Schnittstelle von Host C ist an Port 9 von Switch 1 angeschlossen. Das VLAN Blue ist mit der VID 123 konfiguriert.

Aus der Abbildung geht auch hervor, dass ein Host auch mehreren VLANs angehören kann. Host A hat beispielsweise zwei VLANs, die über die Host-Schnittstelle konfiguriert sind. Die zweite Schnittstelle ist mit VID 456 konfiguriert und an Port 3 mit der gleichen VID angeschlossen. Daher gehört Host A zum VLAN Blue und zum VLAN Yellow.

Während der VLAN-Konfiguration haben Sie den *physikalischen Anschlusspunkt* oder *PPA (Physical Point Of Attachment)* des VLAN angegeben. Zur Berechnung des PPA-Wertes verwenden Sie die folgende Formel:

driver-name `+ VID * 1000 +` *device-instance*

Beachten Sie, dass die Zahl für *Geräteinstanz* kleiner als 1000 sein muss.

Beispielsweise würden Sie den folgenden PPA für eine Schnittstelle `ce1` erstellen, die als Teil des VLAN 456 konfiguriert wurde:

```
ce + 456 * 1000 + 1= ce456001
```

Planen von VLANs in einem Netzwerk

Verwenden Sie das folgende Verfahren, um VLANs für Ihr Netzwerk zu planen.

▼ So planen Sie eine VLAN-Konfiguration

1. **Untersuchen Sie die Topologie des lokalen Netzwerks und prüfen Sie, ob eine Unterteilung in VLANs sinnvoll ist.**

   Ein allgemeines Beispiel einer solchen Topologie finden Sie in Abbildung 6–1.

2. **Erstellen Sie ein Nummerierungsschema für die VIDs und weisen Sie jedem VLAN eine VID zu.**

Hinweis – Eventuell ist bereits ein VLAN-Nummerierungsschema im Netzwerk vorhanden. In diesem Fall müssen Sie die VIDs innerhalb des bestehenden VLAN-Nummerierungsschemas erstellen.

---

3. **Stellen Sie für jedes System fest, welche Schnittstellen Mitglieder eines bestimmten VLAN sein sollen.**

   a. **Stellen Sie fest, welche Schnittstellen derzeit auf dem System konfiguriert sind.**

   ```
   # dladm show-link
   ```

   b. **Legen Sie fest, welche VID jedem Datenlink des Systems zugewiesen werden soll.**

   c. **Erstellen Sie PPAs für jede Schnittstelle, die mit einem VLAN konfiguriert werden soll.**

   Nicht alle Schnittstellen eines Systems müssen unbedingt für das gleiche VLAN konfiguriert werden.

4. **Prüfen Sie die Verbindungen der Schnittstellen mit den Netzwerk-Switches.**

   Notieren Sie die VID jeder Schnittstelle und den Switch-Port, mit dem die Schnittstelle verbunden ist.

5. **Konfigurieren Sie jeden Port des Switches mit der gleichen VID wie die Schnittstelle, mit der der Port verbunden ist.**

   Konfigurationshinweise entnehmen Sie bitte der Dokumentation des Switch-Herstellers.

Konfiguration von VLANs

Hinweis – Wenn Sie Solaris 10 3/05 verwenden, lesen Sie „Konfiguration von VLANs (nur Solaris 10 3/05)“ auf Seite 152.

Oracle Solaris unterstützt jetzt VLANs auf den folgenden Schnittstellentypen:

- `ce`
- `bge`
- `xge`
- `e1000g`

Von den Legacy-Schnittstellentypen kann nur die Schnittstelle ce ein Mitglied eines VLAN werden. Sie können Schnittstellen unterschiedlicher Typen im gleichen VLAN konfigurieren.

Hinweis – Sie können mehrere VLANs in einer IPMP-Gruppe zusammenfassen. Weitere Informationen zu IPMP-Gruppen finden Sie unter „IPMP-Schnittstellenkonfigurationen“ auf Seite 787.

▼ So konfigurieren Sie ein VLAN

Wenn Sie Solaris 10 3/05 verwenden, führen Sie das Verfahren „So werden statische VLANs konfiguriert (nur Solaris 10 3/05)“ auf Seite 153 aus.

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Ermitteln Sie die auf Ihrem System verwendeten Schnittstellentypen.**

   ```
   # dladm show-link
   ```

   Die Ausgabe zeigt die verfügbaren Schnittstellentypen an:

   ```
   ce0             type: legacy    mtu: 1500       device: ce0
    ce1             type: legacy    mtu: 1500       device: ce1
    bge0            type: non-vlan  mtu: 1500       device: bge0
    bge1            type: non-vlan  mtu: 1500       device: bge1
    bge2            type: non-vlan  mtu: 1500       device: bge2
   ```

3. **Konfigurieren Sie eine Schnittstelle als Teil eines VLAN.**

   ```
   # ifconfig interface-PPA plumb IP-address up
   ```

Sie können z. B den folgenden Befehl verwenden, um die Schnittstelle `ce1` mit einer neuen IP-Adresse `10.0.0.2` in einem VLAN mit der VID 123 konfigurieren:

```
# ifconfig ce123001 plumb 10.0.0.2
up
```

Hinweis – Sie können den VLANs genau wie anderen Schnittstellen auch IPv4- und IPv6-Adressen zuweisen.

---

4. **(Optional) Damit die VLAN-Einstellungen auch nach einem Neustart beibehalten werden, erstellen Sie eine** `hostname.`*Schnittstellen-PPA***-Datei für jede Schnittstelle, die als Teil eines VLAN konfiguriert wurde.**

```
# cat hostname.interface-PPA
IPv4-address
```

5. **Richten Sie das VLAN-Tagging und die VLAN-Ports auf dem Switch so ein, dass sie sich mit den VLANs übereinstimmen, die Sie auf dem System eingerichtet haben.**

Beispiel 6–3 Konfiguration eines VLAN

In diesem Beispiel wird gezeigt, wie Sie die Geräte `bge1` und `bge2` in einem VLAN mit der VID 123 konfigurieren.

```
# dladm show-link
ce0            type: legacy    mtu: 1500       device: ce0
ce1            type: legacy    mtu: 1500       device: ce1
bge0           type: non-vlan  mtu: 1500       device: bge0
bge1           type: non-vlan  mtu: 1500       device: bge1
bge2           type: non-vlan  mtu: 1500       device: bge2
# ifconfig bge123001 plumb 10.0.0.1 up
# ifconfig bge123002 plumb 10.0.0.2 up
# cat hostname.bge123001   10.0.0.1
# cat hostname.bge123002   10.0.0.2
# ifconfig -a
 lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
         inet 127.0.0.1 netmask ff000000
 bge123001: flags=201000803<UP,BROADCAST,MULTICAST,IPv4,CoS> mtu 1500 index 2
         inet 10.0.0.1 netmask ff000000 broadcast 10.255.255.255
         ether 0:3:ba:7:84:5e
bge123002:flags=201000803 <UP,BROADCAST,MULTICAST,IPv4,CoS> mtu 1500 index 3
         inet 10.0.0.2 netmask ff000000 broadcast 10.255.255.255
         ether 0:3:ba:7:84:5e
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 4
         inet 192.168.84.253 netmask ffffff00 broadcast 192.168.84.255
         ether 0:3:ba:7:84:5e
# dladm show-link
ce0             type: legacy    mtu: 1500       device: ce0
ce1             type: legacy    mtu: 1500       device: ce1
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1
bge2            type: non-vlan  mtu: 1500       device: bge2
```

```
bge123001       type: vlan 123  mtu: 1500       device: bge1
bge123002       type: vlan 123  mtu: 1500       device: bge2
```

Übersicht der Link-Aggregationen

Hinweis – Das ursprüngliche Oracle Solaris 10-Version und frühere Versionen von Oracle Solaris unterstützen keine Linkaggregationen. Um Linkaggregationen für diese früheren Oracle Solaris-Versionen zu erstellen, verwenden Sie das Sun Trunking, das im *Sun Trunking 1.3 Installation and Users Guide* beschrieben wird.

Mit Oracle Solaris können Sie Netzwerkschnittstellen in Linkaggregationen strukturieren. Eine *Linkaggregation* besteht aus mehreren Schnittstellen auf einem System, die als eine logische Einheit konfiguriert wurden. Linkaggregation (auch als *trunking* bezeichnet) ist im IEEE-Linkaggregationsstandard 802.3ad (`http://www.ieee802.org/3/index.html`) definiert.

Der IEEE 802.3ad Link Aggregation Standard stellt eine Methode zum Zusammenfassen der Kapazitäten mehrerer Vollduplex-Ethernet-Links zu einem logischen Link dar. Diese Linkaggregation-Gruppe wird dann so behandelt, als wäre sie tatsächlich ein einzelner Link.

Linkaggregationen weisen die folgenden Eigenschaften auf:

- **Erhöhte Bandbreite** – Die Kapazitäten mehrerer Links werden zu einem logischen Link zusammengefasst.
- **Automatisches Failover/Failback** – Datenverkehr eines ausgefallenen Links wird automatisch von funktionierenden Links in der Aggregation übernommen.
- **Lastenausgleich** – Sowohl eingehender als auch abgehender Datenverkehr wird gemäß der vom Benutzer vorgegebenen Richtlinien für den Lastenausgleich verteilt, z. B. MAC- oder IP-Adressen.
- **Unterstützung für Redundanz** – Zwei Systeme können mit parallelen Aggregationen konfiguriert werden.
- **Verbesserte Verwaltung** – Alle Schnittstellen können als eine Einheit verwaltet werden.
- **Geringere Belastung für den Netzwerk-Adresspool** – Der gesamten Aggregation kann nur einer IP-Adresse zugeordnet werden.

Grundlagen der Linkaggregationen

Die allgemeine Topologie einer Linkaggregation umfasst eine einzelne Aggregation, die aus mehreren physikalischen Schnittstellen besteht. Eine allgemeine Linkaggregation finden Sie im folgenden Situationen:

- Bei Systemen, die eine Anwendung mit verteiltem starkem Datenverkehr ausführen, können Sie eine Aggregation für den Datenverkehr dieser Anwendung reservieren.

- Bei Standorten mit begrenztem IP-Adressraum, der trotzdem eine große Bandbreite erfordert, benötigen Sie nur eine IP-Adresse für eine große Aggregationen an Schnittstellen.
- Bei Standorten, die die Existenz von internen Schnittstellen verbergen müssen, verbirgt die IP-Adresse der Aggregation die darin enthaltenen Schnittstellen gegenüber externen Anwendungen.

Abbildung 6–3 zeigt eine Aggregation für einen Server, der als Host für eine beliebte Website dient. Die Site benötigt hohe Bandbreite für die Abfragen, die Internet-Kunden an den Datenbankserver der Website stellen. Aus Sicherheitsgründen muss die Existenz der einzelnen Schnittstellen auf dem Server vor externen Anwendungen verborgen werden. Die Lösung ist die Aggregation `aggr1` mit der IP-Adresse `192.168.50.32`. Diese Aggregation besteht aus drei Schnittstellen: `bge0` bis `bge2`. Diese Schnittstellen sind für das Senden von Antworten auf die Anfragen der Kunden reserviert. Die Adresse für den abgehenden Paketverkehr von allen Schnittstellen ist die IP-Adresse von `aggr1`, `192.168.50.32`.

ABBILDUNG 6–3 Grundlegende Topologie einer Linkaggregation

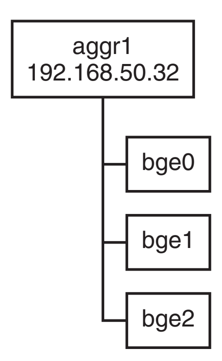
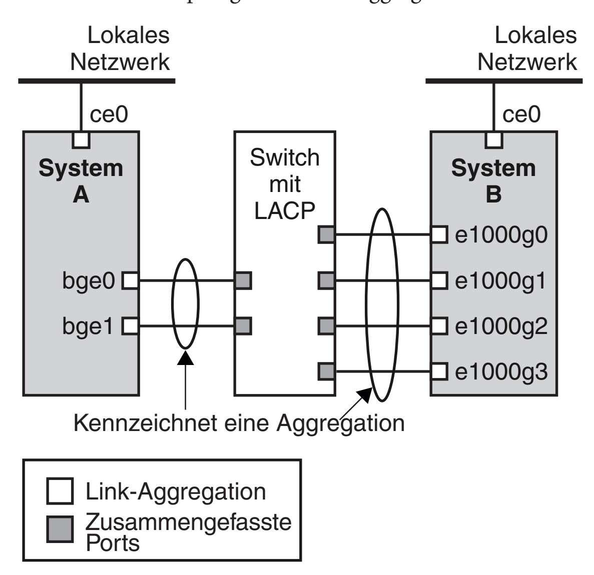


Abbildung 6–4 zeigt ein lokales Netzwerk mit zwei Systemen; auf jedem System ist eine Aggregation konfiguriert. Die beiden Systeme sind über einen Switch miteinander verbunden. Wenn Sie eine Aggregation über einen Switch ausführen, muss dieser Switch die Aggregation-Technologie unterstützen. Dieser Konfigurationstyp eignet sich insbesondere für hoch verfügbare und redundante Systeme.

In der Abbildung verfügt System A über eine Aggregation, die aus den beiden Schnittstellen `bge0` and `bge1` besteht. Diese Schnittstellen sind über zusammengefasste Ports mit dem Switch verbunden. System B verfügt über eine Aggregation mit vier Schnittstellen, `e1000g0` bis `e1000g3`. Auch diese Schnittstellen sind über zusammengefasste Ports auf einem Switch miteinander verbunden.

ABBILDUNG 6–4 Topologie einer Linkaggregation mit Switch



Back-to-Back Linkaggregationen

Die Topologie einer Back-to-Back Linkaggregation umfasst zwei separate Systeme, die – wie in der folgenden Abbildung gezeigt – direkt miteinander verkabelt sind. Die Systeme führen parallele Aggregationen aus.

ABBILDUNG 6–5 Grundlegende Topologie einer Back-to-Back-Aggregation

In dieser Abbildung ist das Gerät `bge0` auf System A direkt mit `bge0` auf System B verbunden, usw. Auf diese Weise unterstützen die Systeme A und B Redundanz und können hohe

Verfügbarkeit und Highspeed-Kommunikation zwischen den beiden Systeme bereitstellen. Jedes System verfügt darüber hinaus über eine Schnittstelle `ce0`, über die der Datenverkehr im lokalen Netzwerk abgewickelt wird.

Die häufigste Anwendung für Back-to-Back-Linkaggregationen sind gespiegelte Datenbankserver. Beide Server müssen gemeinsam aktualisiert werden und erfordern daher beachtliche Bandbreite, Highspeed-Datenverkehr und Zuverlässigkeit. Die häufigste Verwendung für Back-to-Back-Linkaggregationen sind Datencenter.

Richtlinien und Lastenausgleich

Wenn Sie eine Linkaggregation planen, müssen Sie eine Richtlinie für abgehenden Verkehr definieren. Diese Richtlinie kann angeben, wie Pakete über die verfügbaren Links einer Aggregation verteilt werden sollen, um einen Lastenausgleich herzustellen. Im Folgenden sind mögliche Schicht-Bezeichner und deren Wichtigkeit in der Aggregationsrichtlinie aufgeführt:

- **L2** – Legt den abgehenden Link durch Hashing des MAC-Headers (L2) jedes Pakets fest
- **L3** – Legt den abgehenden Link durch Hashing des IP-Headers (L3) jedes Pakets fest
- **L4** – Legt den abgehenden Link durch Hashing des TCP-, UDP- oder eines anderen UDP-Headers (L4) jedes Pakets fest

Darüber hinaus sind alle Kombinationen dieser Richtlinien ebenfalls gültig. Die Standard-Richtlinie ist L4. Weitere Informationen finden Sie in der Manpage `dladm`(1M).

Aggregationsmodi und Switches

Wenn Ihre Aggregationstopologie eine Verbindung über einen Switch umfasst, müssen Sie wissen, ob der Switch das *Link Aggregation Control Protocol (LACP)* unterstützt. Unterstützt der Switch das LACP, müssen Sie LACP für Switch und Aggregation konfigurieren. Sie können jedoch nur einen der folgenden *Modi* definieren, in dem LACP arbeiten soll:

- **Off-Modus** – Der Standardmodus für Aggregationen. LACP-Pakete, die auch als *LACPDUs* bezeichnet werden, werden nicht erzeugt.
- **Active-Modus** – Das System erzeugt in von Ihnen angegebenen, regelmäßigen Intervallen LACPDUs.
- **Passive-Modus** – Das System erzeugt nur dann eine LACPDU, wenn es eine LACPDU vom Switch empfängt. Wenn sowohl Aggregation als auch Switch im Passiv-Modus konfiguriert sind, können Sie keine LACPDUs austauschen.

Informationen zur Syntax finden Sie in der Manpage `dladm`(1M) und der Dokumentation des Switch-Herstellers.

Anforderungen für Linkaggregationen

Ihre Linkaggregationskonfiguration wird durch die folgenden Anforderungen eingeschränkt:

- Sie müssen den Befehl `dladm` zur Konfiguration von Aggregationen verwenden.
- Eine geplumbte (aktivierte) Schnittstelle kann kein Mitglied einer Aggregationen werden.
- Schnittstellen müssen den GLDv3-Typ aufweisen: `xge`, `e1000g` und `bge`.
- Alle Schnittstellen in der Aggregation müssen mit der gleichen Geschwindigkeit und im Vollduplex-Modus ausgeführt werden.
- Sie müssen den Wert für MAC-Adressen im EEPROM-Parameter `local-mac-address?` auf „true" setzen. Anweisungen hierzu finden Sie unter So stellen Sie sicher, dass die MAC-Adresse einer Schnittstelle einmalig ist.

▼ So erstellen Sie eine Linkaggregation

Bevor Sie beginnen

Hinweis – Linkaggregationen arbeiten nur im Vollduplex-Modus in Point-to-Point-Links, die mit identischen Geschwindigkeiten arbeiten. Stellen Sie sicher, dass die Schnittstellen in Ihrer Aggregation dieser Anforderung entsprechen.

Wenn Sie einen Switch in Ihrer Aggregationstopologie verwenden, achten Sie darauf, dass Folgendes auf dem Switch durchgeführt wurde:

- Die Ports müssen für eine Aggregation konfiguriert worden sein
- Wenn der Switch LACP unterstützt, muss LACP entweder im aktiven oder passiven Modus konfiguriert sein

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Stellen Sie fest, welche Schnittstellen derzeit auf dem System installiert sind.**

   ```
   # dladm show-link
   ```

3. **Stellen Sie fest, welche Schnittstellen geplumbt (aktiviert) wurden.**

   ```
   # ifconfig -a
   ```

4. **Erstellen Sie eine Aggregation.**

   ```
   # dladm create-aggr -d interface -d interface [...]key
   ```

Schnittstelle Stellt den Gerätename der Schnittstelle dar, die Teil der Aggregation wird.

Schlüssel Ist die Zahl, mit der die Aggregation gekennzeichnet ist. Die niedrigste Schlüsselzahl ist 1. 0 ist nicht als Schlüssel zugelassen.

Beispiel:

```
# dladm create-aggr -d bge0 -d bge1 1
```

5. **Konfigurieren und plumben (aktivieren) Sie die neu erstellte Aggregation.**

```
# ifconfig aggrkey plumb IP-address up
```

Beispiel:

```
# ifconfig aggr1  plumb 192.168.84.14 up
```

6. **Überprüfen Sie den Status der Aggregation, die Sie gerade erstellt haben.**

```
# dladm show-aggr
```

Die folgende Ausgabe wird angezeigt:

```
key: 1 (0x0001) policy: L4      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby
```

Die Ausgabe zeigt, dass eine Aggregation mit dem Schlüssel 1 und der Richtlinie L4 erstellt wurde.

7. **(Optional) Sorgen Sie dafür, dass die IP-Konfiguration der Linkaggregation auch nach einem Neustart beibehalten wird.**

   a. **Bei Linkaggregationen mit IPv4-Adressen erstellen Sie eine** `/etc/hostname.aggr.`*Schlüssel*-**Datei. Bei IPv6-basierten Linkaggregationen erstellen Sie eine** `/etc/hostname6.aggr.`*Schlüssel*-**Datei.**

   b. **Geben Sie die IPv4- oder IPv6-Adresse der Linkaggregation in die Datei ein.**

   Beispielsweise können Sie die folgende Datei für die in diesem Beispiel erstellte Aggregationen erstellen:

```
# vi /etc/hostname.aggr1
192.168.84.14
```

   c. **Führen Sie einen Neustart durch, um die neue Konfiguration zu übernehmen.**

```
# reboot -- -r
```

d. **Prüfen Sie, ob die in die** `/etc/hostname.aggr`*Schlüssel***-Datei eingegebene Konfiguration einer Linkaggregation konfiguriert wurde.**

```
# ifconfig -a
.
.
aggr1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 192.168.84.14 netmask ff000000 broadcast 192.255.255.
```

Beispiel 6–4 Erstellen einer Linkaggregation

Im folgenden Beispiel werden die Befehle gezeigt, mit denen Sie eine Linkaggregation mit zwei Geräten, `bge0` und `bge1` erstellen. Auch die resultierende Ausgabe wird aufgeführt.

```
# dladm show-link
ce0             type: legacy    mtu: 1500       device: ce0
ce1             type: legacy    mtu: 1500       device: ce1
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1
bge2            type: non-vlan  mtu: 1500       device: bge2
# ifconfig -a
lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.84.253 netmask ffffff00 broadcast 192.168.84.255
        ether 0:3:ba:7:84:5e
# dladm create-aggr -d bge0 -d bge1 1
# ifconfig aggr1 plumb 192.168.84.14 up
# dladm show-aggr
key: 1 (0x0001) policy: L4      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby

# ifconfig -a
lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.84.253 netmask ffffff00 broadcast 192.168.84.255
        ether 0:3:ba:7:84:5e
aggr1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 192.168.84.14 netmask ff000000 broadcast 192.255.255.255
        ether 0:3:ba:7:84:5e
```

Beachten Sie, dass die zwei für die Aggregation verwendeten Schnittstellen nicht zuvor von `ifconfig` geplumbt (aktiviert) wurden.

▼ So bearbeiten Sie eine Aggregation

Im folgenden Verfahren wird gezeigt, wie Sie Änderungen an einer Aggregationsdefinition vornehmen:

- Bearbeiten der Richtlinie der Aggregation
- Ändern des Modus der Aggregation

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Modifizieren Sie die Aggregation, um die Richtlinie zu ändern.

`# dladm modify-aggr -P`*policy key*

Richtlinie Stellt eine oder mehrere der Richtlinien L2, L3 und L4 dar, gemäß der Beschreibung unter „Richtlinien und Lastenausgleich" auf Seite 176.

Schlüssel Ist eine Zahl, die die Aggregation kennzeichnet. Die niedrigste Schlüsselzahl ist 1. 0 ist nicht als Schlüssel zugelassen.

3 Wenn LACP auf dem Switch läuft, dem die Geräte der Aggregation zugewiesen sind, müssen Sie die Aggregation modifizieren, dass LACP unterstützt wird.

Wenn der Switch LACP im passiven Modus ausführt, achten Sie darauf, den aktiven Modus für Ihre Aggregationen zu konfigurieren.

`# dladm modify-aggr -l` *LACP mode* `-t` *timer-value key*

`-l` *LACP-Modus* Gibt den LACP-Modus an, in dem die Aggregation ausgeführt wird. Mögliche Werte sind `active`, `passive` und `off`.

`-t` *Timerwert* Gibt den LACP-Timerwert an, entweder `short` oder `long`.

Schlüssel Ist eine Zahl, die die Aggregation kennzeichnet. Die niedrigste Schlüsselzahl ist 1. 0 ist nicht als Schlüssel zugelassen.

Beispiel 6–5 Bearbeiten einer Linkaggregation

Aus diesem Beispiel geht hervor, wie die Richtlinie der Aggregation `aggr1` in L2 geändert und anschließend der aktive LACP-Modus aktiviert wird.

```
# dladm modify-aggr -P L2 1
# dladm modify-aggr -l active -t short 1
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby
```

▼ So entfernen Sie eine Schnittstelle aus einer Aggregation

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Entfernen Sie eine Schnittstelle aus einer Aggregation.

```
# dladm remove-aggr -d interface
```

Beispiel 6–6 Entfernen von Schnittstellen aus einer Aggregation

Im folgenden Beispiel wird gezeigt, wie Schnittstellen aus der Aggregation `aggr1` entfernt werden.

```
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby
# dladm remove-aggr -d bge1 1
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
```

▼ So löschen Sie eine Aggregation

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Löschen Sie die Aggregation.

```
# dladm delete-aggr key
```

Schlüssel Ist eine Zahl, die die Aggregation kennzeichnet. Die niedrigste Schlüsselzahl ist 1. 0 ist nicht als Schlüssel zugelassen.

Beispiel 6–7 So löschen Sie eine Aggregation

Im folgenden Beispiel wird gezeigt, wie Sie die Aggregation `aggr1` entfernen.

```
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
     device   address           speed     duplex  link    state
# dladm delete-aggr -d 1
```

So konfigurieren Sie VLANs über eine Linkaggregation

Auf die gleiche Weise, in der Sie VLANs über eine Schnittstelle konfigurieren, können Sie sie auch über eine Linkaggregation erstellen. VLANs werden unter „Verwalten von virtuellen lokalen Netzwerken“ auf Seite 167 erläutert. In diesem Abschnitt werden die Konfigurationen für VLANs und Linkaggregationen erläutert.

Bevor Sie beginnen Konfigurieren Sie zuerst die Linkaggregation mit einer gültigen IP-Adresse. Notieren Sie sich den Wert des Aggregations`schlüssels`. Sie benötigen den Wert später bei der Erstellung der VLANs anhand der Aggregation. Hinweise zu Linkaggregationen finden Sie unter „So erstellen Sie eine Linkaggregation“ auf Seite 177.

1. **Wenn bereits zuvor eine Linkaggregation erstellt wurde, fordern Sie den Schlüssel dieser Aggregation an.**

   ```
   # dladm show-aggr
   ```

2. **Erstellen Sie die VLANs anhand der Linkaggregation.**

   `# ifconfig aggr`*VIDkey* `plumb`

   Hierbei gilt:

   VID Die ID des VLAN.

   Schlüssel Der Schlüssel der Linkaggregation, anhand derer das VLAN erstellt wird. Der Schlüssel muss aus drei Ziffern bestehen. Wenn der Aggregationsschlüssel beispielsweise `1` lautet, wird die Nummer im Namen des VLAN als `001` dargestellt.

3. **Wiederholen Sie Schritt 2, um andere VLANs anhand der Aggregation zu erstellen.**

4. **Konfigurieren Sie die VLANs mit gültigen IP-Adressen.**

5. **Fügen Sie zur Erstellung dauerhafter VLAN-Konfigurationen den entsprechenden `/etc/hostname.`*VLAN*-Konfigurationsdateien Angaben zur IP-Adresse hinzu.**

Beispiel 6–8 Konfigurieren mehrerer VLANs über eine Linkaggregation

In diesem Beispiel werden zwei VLANs über eine Linkaggregation konfiguriert. Mit dem `dladm show-aggr`-Befehl wird 1 als Schlüssel der Linkaggregation ermittelt. Den VLANs werden die VIDs 193 und 194 zugewiesen.

```
# dladm show-aggr
key: 1 (0x0001) policy: L4      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby

# ifconfig aggr193001 plumb
# ifconfig aggr193001 192.168.10.5/24 up

# ifconfig aggr194001 plumb
# ifconfig aggr194001 192.168.10.25/24 up

# vi /etc/hostname.aggr193001
192.168.10.5/24

# vi /etc/hostname.aggr194001
192.168.10.25/24
```

KAPITEL 7

Konfigurieren eines IPv6-Netzwerks (Vorgehen)

Dieses Kapitel enthält Aufgaben zur Konfiguration von IPv6 in einem Netzwerk. Folgende Themen werden behandelt:

- „Konfiguration einer IPv6-Schnittstelle“ auf Seite 185
- „Aktivieren von IPv6 auf einer Schnittstelle (Übersicht der Schritte)“ auf Seite 186
- „Konfiguration eines IPv6-Routers“ auf Seite 191
- „Modifizieren einer IPv6-Schnittstellenkonfiguration für Hosts und Server“ auf Seite 196
- „Ändern einer IPv6-Schnittstellenkonfiguration (Übersicht der Schritte)“ auf Seite 196
- „Konfiguration von Tunneln zur Unterstützung von IPv6“ auf Seite 205
- „Aufgaben bei der Konfiguration von Tunneln zur Unterstützung von IPv6 (Übersicht der Schritte)“ auf Seite 204
- „Konfiguration der Namen-Services-Unterstützung für IPv6“ auf Seite 213

Eine Übersicht der IPv6-Konzepte finden Sie in Kapitel 3, „Einführung in IPv6 (Überblick)“. Informationen zu IPv6-Planungsaufgaben finden Sie in Kapitel 4, „Planen eines IPv6-Netzwerks (Aufgaben)“. Referenzinformationen zu den Aufgaben in diesem Kapitel finden Sie in Kapitel 11, „IPv6 im Detail (Referenz)“.

Konfiguration einer IPv6-Schnittstelle

Der erste Schritt bei der IPv6-Konfiguration ist das Aktivieren von IPv6 auf einer Schnittstelle. Sie können IPv6 entweder während der Installation von Oracle Solaris 10 oder durch Konfigurieren von IPv6 auf den Schnittstellen eines installierten Systems aktivieren.

Während der Installation von Oracle Solaris 10 können Sie IPv6 auf einer oder mehreren Schnittstellen eines Systems aktivieren. Nach der Installation sind die folgenden IPv6-bezogenen Dateien und Tabellen gespeichert:

- Jede Schnittstelle, die für IPv6 aktiviert wurde, verfügt über eine zugehörige `/etc/hostname6.`*Schnittstelle*-Datei, z. B. `hostname6.dmfe0`.

- Für Solaris 10 11/06 und frühere Releases wurde die `/etc/inet/ipnodes`-Datei erstellt. Nach der Installation enthält diese Datei in der Regel die IPv6- und IPv4-Loopback-Adressen.
- Die `/etc/nsswitch.conf`-Datei wurde geändert, so dass sie Lookups über IPv6-Adressen aufnehmen kann.
- Die Richtlinientabelle zur IPv6-Adressauswahl wurde erstellt. Diese Tabelle priorisiert das IP-Adressformat für Übertragungen über eine IPv6-konforme Schnittstelle.

In diesem Abschnitt wird beschrieben, wie Sie IPv6 auf den Schnittstellen eines installierten Systems aktivieren.

Aktivieren von IPv6 auf einer Schnittstelle (Übersicht der Schritte)

In der folgenden Tabelle sind die Aufgaben beschrieben, die zum Konfigurieren der IPv6-Schnittstellen erforderlich sind. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen Aufgaben sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
Aktivieren von IPv6 auf einer Schnittstelle eines Systems, auf dem bereits Oracle Solaris 10 installiert ist.	Aktivieren Sie IPv6 auf einer Schnittstelle, nachdem Oracle Solaris 10 installiert wurde.	„So aktivieren Sie eine IPv6-Schnittstelle für die aktuelle Sitzung“ auf Seite 186
Beibehalten der Konfiguration einer IPv6-konformen Schnittstelle auch nach einem Neustart.	Übernehmen Sie die IPv6-Adresse der Schnittstelle permanent.	„So aktivieren Sie persistente IPv6-Schnittstellen“ auf Seite 188
Deaktivieren der automatischen IPv6-Adresskonfiguration.	Konfigurieren Sie die Schnittstellen-ID-Komponente der IPv6-Adresse manuell.	„So deaktivieren Sie die automatische IPv6-Adresskonfiguration“ auf Seite 190

▼ So aktivieren Sie eine IPv6-Schnittstelle für die aktuelle Sitzung

Beginnen Sie die IPv6-Konfiguration, indem Sie IPv6 auf den Schnittstellen aller Systeme aktivieren, die zu IPv6-Knoten werden. Zunächst bezieht die Schnittstelle ihre IPv6-Adresse über den Autokonfigurationsprozess, der unter „Automatische IPv6-Adresskonfiguration“ auf Seite 86 ausführlich beschrieben wird. Dann können Sie die Knotenkonfiguration basierend auf dessen Funktion im IPv6-Netzwerk (Host, Server oder Router) anpassen.

Hinweis – Befindet sich die Schnittstelle auf dem gleichen Link wie der Router, der derzeit einen IPv6-Präfix bekannt gibt, bezieht die Schnittstelle dieses Standortpräfix als Teil der automatisch konfigurierten Adressen. Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie einen IPv6-konformen Router" auf Seite 192.

Im folgenden Verfahren wird erklärt, wie Sie IPv6 für eine Schnittstelle aktivieren, die nach der Installation von Oracle Solaris 10 hinzugefügt wurde.

Bevor Sie beginnen Schließen Sie zunächst alle Planungsaufgaben für ein IPv6-Netzwerk, z. B. das Aufrüsten von Hard- und Software und die Vorbereitungen für einen Adressierungsplan ab. Weitere Informationen finden Sie unter „Planung der Einführung von IPv6 (Übersicht der Schritte)" auf Seite 89.

1. **Melden Sie sich auf dem künftigen IPv6-Knoten als Primäradministrator oder als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Aktivieren Sie IPv6 auf einer Schnittstelle.**

   ```
   # ifconfig inet6 interface plumb up
   ```

3. **Starten Sie den IPv6-Daemon `in.ndpd`.**

   ```
   # /usr/lib/inet/in.ndpd
   ```

Hinweis – Sie können den Status der IPv6-konformen Schnittstellen eines Knotens mit dem Befehl `ifconfig-a6` anzeigen.

Beispiel 7–1

Aktivieren einer IPv6-Schnittstelle nach der Installation

Im folgenden Beispiel wird gezeigt, wie Sie IPv6 auf der Schnittstelle `qfe0` aktivieren. Bevor Sie beginnen, prüfen Sie den Status aller im System konfigurierten Schnittstellen.

```
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
qfe0: flags=1000863 <UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500
           index 2
        inet 172.16.27.74 netmask ffffff00 broadcast 172.16.27.255
        ether 0:3:ba:13:14:e1
```

Derzeit ist nur die Schnittstelle `qfe0` für dieses System konfiguriert. Aktivieren Sie IPv6 auf dieser Schnittstelle wie folgt:

```
# ifconfig inet6 qfe0 plumb up
# /usr/lib/inet/in.ndpd
# ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 0:3:ba:13:14:e1
        inet6 fe80::203:baff:fe13:14e1/10
```

Das Beispiel zeigt den Status der Systemschnittstelle vor und nachdem `qfe0` für IPv6 aktiviert wurde. Mit der Option `-a6` des Befehls `ifconfig` zeigen Sie nur die IPv6-Informationen für `qfe0` und die Loopback-Schnittstelle an. Die Ausgabe deutet darauf hin, dass nur eine Link-lokale Adresse für `qfe0` konfiguriert wurde: `fe80::203:baff:fe13:14e1/10`. Diese Adresse deutet darauf hin, dass noch kein Router auf dem lokalen Link des Knotens einen Standortpräfix bekannt gibt.

Nachdem IPv6 aktiviert wurde, können Sie mit dem Befehl `ifconfig -a` die IPv4- und IPv6-Adressen aller Schnittstellen im System anzeigen.

Nächste Schritte

- Zur Konfiguration des IPv6-Knoten als Router lesen Sie „Konfiguration eines IPv6-Routers“ auf Seite 191.
- Zum Beibehalten der IPv6-Schnittstellenkonfiguration nach einem Neustart lesen Sie „So aktivieren Sie persistente IPv6-Schnittstellen“ auf Seite 188.
- Zum Deaktivieren der automatischen Adresskonfiguration auf einem Knoten lesen Sie „So deaktivieren Sie die automatische IPv6-Adresskonfiguration“ auf Seite 190.
- Zum Anpassen des Knotens als ein Server lesen Sie die Vorschläge unter „Verwaltung von IPv6-konformen Schnittstellen auf Servern“ auf Seite 202.

▼ So aktivieren Sie persistente IPv6-Schnittstellen

Im folgenden Verfahren wird beschrieben, wie die Konfiguration von automatisch konfigurierten IPv6-Adressen auch nach einem Neustart beibehalten wird.

Hinweis – Befindet sich die Schnittstelle auf dem gleichen Link wie der Router, der derzeit einen IPv6-Präfix bekannt gibt, bezieht die Schnittstelle dieses Standortpräfix als Teil der automatisch konfigurierten Adressen. Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie einen IPv6-konformen Router“ auf Seite 192.

---

1. **Melden Sie sich auf dem IPv6-Knoten als Primäradministrator oder als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie IPv6-Adressen für Schnittstellen, die nach der Installation hinzugefügt wurden.

a. Erstellen Sie die Konfigurationsdatei.

```
# touch /etc/hostname6.interface
```

b. Fügen Sie Adressen zur Konfigurationsdatei hinzu.

```
inet6 ipv6-address up
addif inet6 ipv6-address up
...
```

3 Erstellen Sie eine statische IPv6-Standardroute.

```
# /usr/sbin/route -p add -inet6 default ipv6-address
```

4 (Optional) Erstellen Sie eine `/etc/inet/ndpd.conf`-Datei, mit der die Parameter der Schnittstellenvariablen auf dem Knoten definiert werden.

Wenn Sie temporäre Adressen für die Schnittstelle des Hosts erstellen müssen, lesen Sie „Verwenden von temporären Adressen für eine Schnittstelle" auf Seite 196. Weitere Informationen zur `/etc/inet/ndpd.conf`-Datei finden Sie in der Manpage `ndpd.conf(4)` und unter „`ndpd.conf`-Konfigurationsdatei" auf Seite 284.

5 Starten Sie den Knoten neu.

```
# reboot -- -r
```

Der Neustartprozess sendet Pakete zur Router-Erkennung. Wenn ein Router mit einem Standortpräfix antwortet, kann der Knoten eine Schnittstelle mit einer zugehörigen `/etc/hostname6.`*Schnittstelle*-Datei mit einer globalen IPv6-Adresse konfigurieren. Andernfalls werden die IPv6-konformen Schnittstellen ausschließlich mit Link-lokalen Adressen konfiguriert. Durch den Neustart werden auch der `in.ndpd`- und anderen Netzwerkdaemons im IPv6-Modus neugestartet.

Beispiel 7–2 Beibehalten der Konfiguration einer IPv6-Schnittstelle nach einem Neustart

Im folgenden Beispiel wird gezeigt, wie die Konfiguration der IPv6-Schnittstelle `qfe0` auch nach einem Neustart beibehalten wird. In diesem Beispiel gibt ein Router das Standortpräfix und die Teilnetz-ID `2001:db8:3c4d:15/64`auf dem lokalen Link bekannt.

Zunächst prüfen Sie den Status der Systemschnittstellen.

```
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
qfe0: flags=1000863 <UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500
           index 2
        inet 172.16.27.74 netmask ffffff00 broadcast 172.16.27.255
        ether 0:3:ba:13:14:e1
```

```
# touch /etc/hostname6.qfe0
# vi /etc/hostname6.qfe0
inet6 fe80::203:baff:fe13:1431/10 up
addif inet6 2001:db8:3c4d:15:203:baff:fe13:14e1/64 up

# route -p add -inet6 default fe80::203:baff:fe13:1431
# reboot -- -r
```

Prüfen Sie, ob die von Ihnen konfigurierte IPv6-Adresse der Schnittstelle `qfe0` noch immer zugewiesen ist.

```
# ifconfig -a6
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
       ether 0:3:ba:13:14:e1
       inet6 fe80::203:baff:fe13:14e1/10
 qfe0:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500
          index 2
        inet6 2001:db8:3c4d:15:203:baff:fe13:14e1/64
```

Die Ausgabe des Befehls `ifconfig -a6` zeigt zwei Einträge für `qfe0`. Der standardmäßige `qfe0`-Eintrag enthält die MAC- sowie die Link-lokale Adresse. Der zweite Eintrag `qfe0:1` gibt eine Pseudo-Schnittstelle an, die für die zusätzliche IPv6-Adresse auf der Schnittstelle`qfe0` erstellt wurde. Die neue, globale IPv6-Adresse `2001:db8:3c4d:15:203:baff:fe13:14e1/64` enthält den vom lokalen Router bekannt gegebenen Standortpräfix und die Teilnetz-ID.

Nächste Schritte

- Zur Konfiguration des neuen IPv6-Knotens als Router lesen Sie „Konfiguration eines IPv6-Routers“ auf Seite 191.
- Zum Deaktivieren der automatischen Adresskonfiguration auf einem Knoten lesen Sie „So deaktivieren Sie die automatische IPv6-Adresskonfiguration“ auf Seite 190.
- Zum Anpassen des neuen Knotens als einen Server lesen Sie die Vorschläge unter „Verwaltung von IPv6-konformen Schnittstellen auf Servern“ auf Seite 202.

▼ So deaktivieren Sie die automatische IPv6-Adresskonfiguration

Im Allgemeinen verwenden Sie die automatische Adresskonfiguration zum Erzeugen der IPv6-Adressen für die Schnittstellen der Hosts und Server. Manchmal möchten Sie jedoch die automatische Adresskonfiguration deaktivieren, insbesondere dann, wenn ein Token manuell konfiguriert werden muss. Dieser Vorgang wird unter „Konfiguration eines IPv6-Tokens“ auf Seite 200 beschrieben.

1. **Melden Sie sich auf dem IPv6-Knoten als Primäradministrator oder als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie eine `/etc/inet/ndpd.conf`-Datei für den Knoten.

Die `/etc/inet/ndpd.conf`-Datei definiert die Schnittstellenvariablen für einen bestimmten Knoten. Diese Datei sollte den folgenden Inhalt aufweisen, damit die automatische Adresskonfiguration für alle Schnittstellen eines Servers deaktiviert wird:

```
if-variable-name StatelessAddrConf false
```

Weitere Informationen zur `/etc/inet/ndpd.conf`-Datei finden Sie in der Manpage `ndpd.conf(4)` und unter „`ndpd.conf`-Konfigurationsdatei" auf Seite 284.

3 Aktualisieren Sie den IPv6-Daemon mit Ihren Änderungen.

```
# pkill -HUP in.ndpd
```

Konfiguration eines IPv6-Routers

Der erste Schritt bei der Konfiguration von IPv6 in einem Netzwerk ist das Konfigurieren von IPv6 auf einem Router. Zur Router-Konfiguration gehören mehrere, unabhängig voneinander auszuführende Aufgaben, die in diesem Abschnitt beschrieben werden. Abhängig von den Anforderungen Ihres Standorts können Sie einige oder alle Aufgaben durchführen.

Konfiguration eines IPv6-Routers (Übersicht der Schritte)

Führen Sie die in der folgenden Tabelle aufgeführten Aufgaben in der angegebenen Reihenfolge aus, um das IPv6-Netzwerk zu konfigurieren. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen Aufgaben sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
1. Bevor Sie mit der IPv6-Konfiguration beginnen, stellen Sie sicher, dass alle Voraussetzungen erfüllt sind.	Bevor Sie einen IPv6-konformen Router konfigurieren können, müssen Sie alle Planungsaufgaben und die Installation von Oracle Solaris auf IPv6-konformen Schnittstellen abgeschlossen haben.	Kapitel 4, „Planen eines IPv6-Netzwerks (Aufgaben)" und „Konfiguration einer IPv6-Schnittstelle" auf Seite 185.
2. Konfiguration eines Routers.	Definieren Sie das Standortpräfix für das Netzwerk.	„So konfigurieren Sie einen IPv6-konformen Router" auf Seite 192

Aufgabe	Beschreibung	Siehe
3. Konfiguration der Tunnelschnittstellen auf dem Router.	Richten Sie manuell einen Tunnel oder eine 6to4-Tunnelschnittstelle auf dem Router ein. Das lokale IPv6-Netzwerk benötigt Tunnel, um mit anderen, isolierten IPv6-Netzwerken kommunizieren zu können.	■ „So konfigurieren Sie einen 6to4-Tunnel“ auf Seite 208 ■ „So konfigurieren Sie einen IPv6-über-IPv4-Tunnel“ auf Seite 205 ■ „So konfigurieren Sie einen IPv6-über-IPv6-Tunnel“ auf Seite 206 ■ „So konfigurieren Sie einen IPv4-über-IPv6-Tunnel“ auf Seite 207
4. Konfiguration der Switches im Netzwerk.	Wenn Ihre Netzwerkkonfiguration Switches umfasst, konfigurieren Sie diese jetzt für IPv6.	Lesen Sie dazu die Dokumentation des Switch-Herstellers.
5. Konfiguration aller Hubs im Netzwerk.	Wenn Ihre Netzwerkkonfiguration Hubs umfasst, konfigurieren Sie diese jetzt für IPv6.	Lesen Sie dazu die Dokumentation des Hub-Herstellers.
6. Konfiguration des Netzwerk-Namen-Services für IPv6.	Konfigurieren Sie Ihren primären Namen-Service (DNS, NIS oder LDAP), so dass IPv6-Adressen erkannt werden, nachdem der Router für IPv6 konfiguriert wurde.	„So fügen Sie IPv6-Adressen zum DNS hinzu“ auf Seite 214
7. (Optional) Ändern der Adressen der IPv6-konformen Schnittstellen auf Hosts und Servern.	Nach der Konfiguration des Routers für IPv6 nehmen Sie Änderungen auf den IPv6-konformen Hosts und Routern vor.	„Modifizieren einer IPv6-Schnittstellenkonfiguration für Hosts und Server“ auf Seite 196
Konfiguration der Anwendungen zur Unterstützung von IPv6	Verschiedene Anwendungen benötigen unterschiedliche Maßnahmen, damit sie IPv6 unterstützen.	Lesen Sie dazu die Dokumentation der Anwendungen

▼ So konfigurieren Sie einen IPv6-konformen Router

Hierbei wird angenommen, dass alle Schnittstellen des Routers während der Oracle Solaris-Installation für IPv6 konfiguriert wurden.

1 Nehmen Sie auf dem System, das als IPv6-Router konfiguriert werden soll, die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Prüfen Sie, welche Schnittstellen auf dem Router während der Installation für IPv6 konfiguriert wurden.

```
# ifconfig -a
```

Prüfen Sie in der Ausgabe, ob die Schnittstellen, die Sie für IPv6 konfigurieren möchten, derzeit mit Link-lokalen Adressen geplumbt (aktiviert) sind. Die folgende Beispielausgabe des Befehls `ifconfig -a` zeigt die IPv4- und IPv6-Adressen, die für die Schnittstellen des Routers konfiguriert wurden.

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
dmfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 172.16.26.232 netmask ffffff00 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:15
dmfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4 mtu 1500 index 3
        inet 172.16.26.220 netmask ffffff00 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:16
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
dmfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 0:3:ba:11:b1:15
        inet6 fe80::203:baff:fe11:b115/10
dmfe1: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 3
        ether 0:3:ba:11:b1:16
        inet6 fe80::203:baff:fe11:b116/10
```

Außerdem zeigt die Ausgabe, dass die primäre Netzwerkschnittstelle `dmfe0` und die zusätzliche Schnittstelle `dmfe1` während der Installation mit den link–local-IPv6-Adressen `fe80::203:baff:fe11:b115/10` und `fe80::203:baff:fe11:b116/10` konfiguriert wurden.

3 Konfigurieren Sie für alle Schnittstellen des Routers die IPv6-Paketweiterleitung.

Unter Solaris 10 11/03 und früheren Releases verwenden Sie den folgenden Befehl:

```
# routeadm -e ipv6-forwarding -u
```

Verwenden Sie eine der folgenden Optionen, um die Paketweiterleitung zu aktivieren:

- Verwenden Sie entweder den `routeadm`-Befehl:

  ```
  # routeadm -e ipv6-forwarding -u
  ```
- Oder verwenden Sie den folgenden Service Management Facility (SMF)-Befehl:

  ```
  # svcadm enable ipv6-forwarding
  ```

4 Starten Sie den Routing-Daemon.

Der `in.ripngd`-Daemon wickelte das IPv6-Routing ab.

Unter Solaris 10 11/06 und früheren Releases starten Sie den `in.ripngd`-Daemon durch Eingabe des folgenden Befehls:

```
# routeadm -e ipv6-routing
# routeadm -u
```

Aktivieren Sie das IPv6-Routing mit einer der folgenden Optionen:

- Geben Sie den `routeadm`-Befehl ein:

```
# routeadm -e ipv6-routing -u
```

- Oder verwenden Sie die SMF zum Aktivieren des IPv6-Routings:

```
# svcadm enable ripng:default
```

Informationen zur Syntax des `routeadm`-Befehls finden Sie in der Manpage `routeadm(1M)`.

5. **Erstelle Sie die Datei `/etc/inet/ndpd.conf`.**

   Sie geben das vom Router bekannt zu gebende Standortpräfix und andere Konfigurationsinformationen in die Datei `/etc/inet/ndpd.conf` einn. Diese Datei wird vom `in.ndpd`-Daemon eingelesen, der das IPv6 Neighbor Discovery-Protokoll implementiert.

   Eine Liste der Variablen und zulässigen Werte finden Sie unter „`ndpd.conf`-Konfigurationsdatei“ auf Seite 284 und in der Manpage `ndpd.conf(4)`.

6. **Geben Sie den folgenden Text in die `/etc/inet/ndpd.conf`-Datei ein:**

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

   Dieser Text weist den `in.ndpd`-Daemon an, die Router Advertisement-Nachrichten über alle Schnittstellen des Routers zu senden, die für IPv6 konfiguriert wurden.

7. **Fügen Sie in die Datei `/etc/inet/ndpd.conf` zusätzlichen Text ein, um das Standortpräfix der verschiedenen Router-Schnittstellen zu konfigurieren.**

   Der Text muss das folgende Format aufweisen:

   `prefix` *global-routing-prefix*`:`*subnet ID*`/64` *interface*

   Die folgende `/etc/inet/ndpd.conf`-Beispieldatei konfiguriert den Router zur Bekanntgabe des Standortpräfix `2001:0db8:3c4d::/48` über die Schnittstellen `dmfe0` und `dmfe1`.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on

if dmfe0 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:15::0/64 dmfe0

if dmfe1 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:16::0/64 dmfe1
```

8. **Starten Sie das System neu.**

   Der IPv6-Router sendet auf dem lokalen Link Advertisement-Nachrichten mit allen Standortpräfixen, die in der `ndpd.conf`-Datei enthalten sind.

Beispiel 7–3 `ifconfig`-Ausgabe zeigt IPv6-Schnittstellen

Im folgenden Beispiel wird die Ausgabe des `ifconfig - a`-Befehls gezeigt, die Sie nach Abschluss des Verfahrens unter „Konfiguration eines IPv6-Routers“ auf Seite 191 erhalten.

```
lo0: flags=1000849 <UP LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
dmfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 172.16.15.232 netmask ffffff00 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:15
dmfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4 mtu 1500 index 3
        inet 172.16.16.220 netmask ffffff00 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:16
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
dmfe0: flags=2100841 <UP,RUNNING,MULTICAST,ROUTER,IPv6> mtu 1500 index 2
        ether 0:3:ba:11:b1:15
        inet6 fe80::203:baff:fe11:b115/10
dmfe0:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6> mtu 1500
          index 2
        inet6 2001:db8:3c4d:15:203:baff:fe11:b115/64
dmfe1: flags=2100841 <UP,RUNNING,MULTICAST,ROUTER,IPv6> mtu 1500 index 3
        ether 0:3:ba:11:b1:16
        inet6 fe80::203:baff:fe11:b116/10
dmfe1:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6> mtu 1500
           index 3
        inet6 2001:db8:3c4d:16:203:baff:fe11:b116/64
```

In diesem Beispiel weist jede für IPv6 konfigurierte Schnittstelle jetzt zwei Adressen auf. Der Eintrag mit dem Namen der Schnittstelle, z. B. `dmfe0`, zeigt die Link-lokale Adresse dieser Schnittstelle an. Der Eintrag im Format *Schnittstelle:n*, z. B. `dmfe0:1`, zeigt eine globale IPv6-Adresse an. Diese Adresse enthält neben der Schnittstellen-ID das Standortpräfix, das Sie in der `/etc/ndpd.conf`-Datei konfiguriert haben.

Siehe auch

- Informationen zur Konfiguration von Tunneln von Routern, die Sie in Ihrer IPv6-Netzwerktopologie angegeben haben, finden Sie unter „Konfiguration von Tunneln zur Unterstützung von IPv6“ auf Seite 205.
- Informationen zur Konfiguration von Switches und Hubs in Ihrem Netzwerk entnehmen Sie bitte der Dokumentation der Hersteller.
- Informationen zur Konfiguration von IPv6-Hosts finden Sie unter „Modifizieren einer IPv6-Schnittstellenkonfiguration für Hosts und Server“ auf Seite 196.
- Informationen zur Verbesserung der IPv6-Unterstützung auf Servern finden Sie unter „Verwaltung von IPv6-konformen Schnittstellen auf Servern“ auf Seite 202.
- Ausführliche Informationen zu den IPv6-Befehlen, -Dateien und -Daemons finden Sie unter „Oracle Solaris 10 IPv6-Implementierung“ auf Seite 284.

Modifizieren einer IPv6-Schnittstellenkonfiguration für Hosts und Server

In diesem Abschnitt wird beschrieben, wie Sie die Konfiguration von IPv6-konformen Schnittstellen auf Knoten modifizieren, bei denen es sich um Hosts oder Server handelt. In den meisten Fällen müssen Sie die automatische Adresskonfiguration für IPv6-konforme Schnittstellen verwenden, die unter „Einführung in die statusfreie automatische Konfiguration" auf Seite 86 beschrieben wird. Sie können die IPv6-Adresse einer Schnittstelle jedoch auch ändern. Dies wird im Rahmen der Aufgaben in diesem Abschnitt beschrieben.

Ändern einer IPv6-Schnittstellenkonfiguration (Übersicht der Schritte)

In der folgenden Tabelle sind die Aufgaben beschrieben, die zum Modifizieren eines vorhandenen IPv6-Netzwerks erforderlich sind. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
Deaktivieren der automatischen IPv6-Adresskonfiguration.	Konfigurieren Sie die Schnittstellen-ID-Komponente der IPv6-Adresse manuell.	„So deaktivieren Sie die automatische IPv6-Adresskonfiguration" auf Seite 190
Erstellen einer temporären Adresse für einen Host.	Verbergen Sie die Schnittstellen-ID eines Hosts, indem Sie eine zufällig erstellte temporärer Adresse konfigurieren, die als die niedrigeren 64 Bit der Adresse verwendet wird.	„So konfigurieren Sie eine temporäre Adresse" auf Seite 197
Konfiguration eines Tokens für die Schnittstellen-ID eines Systems.	Erstellen Sie ein 64-Bit-Token, das als Schnittstellen-ID in einer IPv6-Adresse verwendet wird.	„So konfigurieren Sie ein benutzerdefiniertes IPv6-Token" auf Seite 200

Verwenden von temporären Adressen für eine Schnittstelle

Eine *temporäre IPv6-Adresse* enthält anstelle der MAC-Adresse der Schnittstelle eine zufällig erzeugte 64-Bit-Zahl als Schnittstellen-ID. Temporäre Adressen können Sie für alle Schnittstellen auf einem IPv6-Knoten verwenden, die anonym bleiben sollen. So möchten Sie

eventuell temporäre Adressen für die Schnittstellen eines Hosts verwenden, der auf öffentliche Webserver zugreifen muss. Temporäre Adressen implementieren die IPv6-Verbesserungen zur Privatsphäre. Diese Erweiterungen sind in RFC 3041 unter „Privacy Extensions for Stateless Address Autoconfiguration in IPv6" (`http://www.ietf.org/rfc/rfc3041.txt?number=3041`) beschrieben.

Falls erforderlich, aktivieren Sie eine temporäre Adresse für eine oder mehrere Schnittstellen in der `/etc/inet/ndpd.conf`-Datei. Im Gegensatz zu standardmäßigen, automatisch konfigurierten IPv6-Adressen besteht eine temporäre Adresse aus dem 64-Bit-Teilnetzpräfix einer zufällig erzeugten 64-Bit-Zahl. Diese Zufallszahl wird zur Schnittstellen-ID-Komponente der IPv6-Adresse. Mit einer temporären Adresse als Schnittstellen-ID wird keine Link-lokale Adresse erzeugt.

Beachten Sie, dass temporäre Adressen standardmäßig eine *bevorzugte Lebensdauer* von einem Tag haben. Wenn Sie das Erzeugen von temporären Adressen aktivieren, müssen Sie auch die folgenden Variablen in der `/etc/inet/ndpd.conf`-Datei konfigurieren:

gültige Lebensdauer TmpValidLifetime
: Zeit, über die die temporäre Adresse existiert; danach wird sie vom Host gelöscht.

bevorzugte Lebensdauer TmpPreferredLifetime
: Verstrichene Zeit, bevor die temporäre Adresse eingestellt wird. Diese Zeit muss kürzer als die gültige Lebensdauer sein.

Adressregenerierung
: Zeit vor dem Ablauf der bevorzugten Lebensdauer, während der der Host eine neue temporäre Adresse generieren muss.

Sie drücken die Zeit für temporäre Adressen wie folgt aus:

n
: *n* Anzahl an Sekunden, die Standardeinstellung

n `h`
: *n* Anzahl an Stunden (`h`)

n `d`
: *n* Anzahl an Tagen (`d`)

▼ So konfigurieren Sie eine temporäre Adresse

1. **Melden Sie sich auf dem IPv6-Host als Primäradministrators oder als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Falls erforderlich, aktivieren Sie IPv6 auf den Schnittstellen des Hosts.**

   Lesen Sie dazu „So aktivieren Sie eine IPv6-Schnittstelle für die aktuelle Sitzung“ auf Seite 186.

3. **Bearbeiten Sie die `/etc/inet/ndpd.conf`-Datei, um das Erzeugen von temporären Adressen zu aktivieren.**

- Um auf allen Schnittstellen eines Hosts temporäre Adressen zu konfigurieren, fügen Sie die folgende Zeile in die `/etc/inet/ndpd.conf`-Datei ein:

  `ifdefault TmpAddrsEnabled true`
- Um für eine bestimmte Schnittstelle eine temporäre Adresse zu konfigurieren, fügen Sie die folgende Zeile in die `/etc/inet/ndpd.conf`-Datei ein:

  `if` *interface* **`TmpAddrsEnabled true`**

4 (Optional) Geben Sie die gültige Lebensdauer für die temporäre Adresse ein.

`ifdefault TmpValidLifetime` *duration*

Diese Syntax gibt die gültige Lebensdauer aller Schnittstellen auf einem Host an. Der Wert für *Dauer* muss in Sekunden, Stunden oder Tagen angegeben sein. Die standardmäßige gültige Lebensdauer beträgt 7 Tage. Alternativ können Sie `TmpValidLifetime` mit den Schlüsselwörtern `if` *Schnittstelle* verwenden, um die gültige Lebensdauer für eine temporäre Adresse einer bestimmten Schnittstelle anzugeben.

5 (Optional) Geben Sie die bevorzugte Lebensdauer für eine temporäre Adresse ein, nach deren Ablauf die Adresse ungültig wird.

`if` *interface* **`TmpPreferredLifetime`** *duration*

Diese Syntax gibt die bevorzugte Lebensdauer für die temporäre Adresse einer bestimmten Schnittstelle an. Die standardmäßige bevorzugte Lebensdauer beträgt ein Tag. Alternativ können Sie `TmpPreferredLifetime` mit dem Schlüsselwort `ifdefault` verwenden, um die bevorzugte Lebensdauer für die temporären Adressen aller Schnittstellen auf einem Host anzugeben.

Hinweis – Die Standard-Adressauswahl gibt abgelaufenen IPv6-Adressen eine niedrigere Priorität. Wenn eine temporäre IPv6-Adresse abläuft, wählt die Standard-Adressauswahl eine nicht-abgelaufene Adresse als Quelladresse eines Pakets. Eine nicht-abgelaufene Adresse könnte die automatisch erzeugte IPv6-Adresse oder sogar die IPv4-Adresse der Schnittstelle sein. Weitere Informationen zur Standard-Adressauswahl finden Sie unter „Verwaltuen der standardmäßigen Adressauswahl“ auf Seite 242.

---

6 (Optional) Geben Sie eine Vorlaufzeit vor der Ablaufzeit der Adresse ein, während der der Host eine neue temporäre Adresse erzeugen muss.

`ifdefault TmpRegenAdvance duration`

Diese Syntax gibt die Vorlaufzeit vor dem Ablauf der temporären Adressen aller Schnittstellen auf einem Host an. Der Standardwert beträgt 5 Sekunden.

7 Ändern Sie die Konfiguration des `in.ndpd`-Daemon.

```
# pkill -HUP in.ndpd
# /usr/lib/inet/in.ndpd
```

8 **Prüfen Sie, ob die temporären Adressen erstellt wurden, indem Sie – wie in** `Example&;7—5` **gezeigt – den Befehl** `-ifconfig` **Beispiel 7–5 ausführen.**

Die Ausgabe des Befehls `ifconfig` muss das Wort `TEMPORARY` in der gleichen Zeile wie die Schnittstellendefinition enthalten.

Beispiel 7–4 Temporäre Adressvariablen in der `/etc/inet/ndpd.conf`-Datei

Im folgenden Beispiel wird ein Segment einer `/etc/inet/ndpd.conf`-Datei gezeigt, in dem die temporären Adressen für die primären Netzwerkschnittstelle aktiviert sind.

```
ifdefault TmpAddrsEnabled true

ifdefault TmpValidLifetime 14d

ifdefault TmpPreferredLifetime 7d

ifdefault TmpRegenAdvance 6s
```

Beispiel 7–5 `ifconfig-a6`-Befehlsausgabe mit aktivierten temporären Adressen

Das folgende Beispiel zeigt die Ausgabe des `ifconfig`-Befehls, nachdem die temporären Adressen erstellt wurden.

```
# ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
     inet6 ::1/128
hme0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
     ether 8:0:20:b9:4c:54
     inet6 fe80::a00:20ff:feb9:4c54/10
hme0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
     inet6 2001:db8:3c4d:15:a00:20ff:feb9:4c54/64
hme0:2: flags=802080841<UP,RUNNING,MULTICAST,ADDRCONF,IPv6,TEMPORARY> mtu 1500 index 2
      inet6 2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64
```

Beachten Sie, dass die Zeile nach der Schnittstelle `hme0:2` das Wort `TEMPORARY` enthält. Diese Zuweisung kennzeichnet, dass die Adresse `2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64` über eine temporäre Schnittstellen-ID verfügt.

Siehe auch

- Informationen zum Einrichten der Namen-Services-Unterstützung für IPv6-Adressen finden Sie unter „Konfiguration der Namen-Services-Unterstützung für IPv6“ auf Seite 213.
- Informationen zur Konfiguration von IPv6-Adressen für einen Server finden Sie unter „So konfigurieren Sie ein benutzerdefiniertes IPv6-Token“ auf Seite 200.
- Informationen zur Überwachung der Aktivitäten auf IPv6-Knoten finden Sie in Kapitel 8, „Verwaltung eines TCP/IP-Netzwerks (Aufgaben)“.

Konfiguration eines IPv6-Tokens

Die 64-Bit-Schnittstellen-ID einer IPv6-Adresse wird auch als *Token* bezeichnet. Lesen Sie dazu „Einführung in die IPv6-Adressierung“ auf Seite 78. Während der automatischen Adresskonfiguration wird das Token der MAC-Adresse der Schnittstelle zugeordnet. Meistens verwenden nicht-routende Knoten, das heißt IPv6-Hosts und -Server, ihre automatisch konfigurierten Token.

Das Verwenden von automatisch konfigurierten Token kann jedoch ein Problem für Server darstellen, deren Schnittstellen im Rahmen der Systemwartung gewechselt werden. Wenn eine Schnittstellenkarte ausgetauscht wird, ändert sich auch die MAC-Adresse. Dies kann bei Servern, die von stabilen IP-Adressen abhängig sind, zu Problemen führen. Verschiedene Teile der Netzwerkinfrastruktur, z. B. DNS oder NIS, haben eventuell bestimmte IPv6-Adressen für die Schnittstellen des Servers gespeichert.

Um Probleme bei Adressänderungen zu vermeiden, können Sie manuell ein Token konfigurieren, das als Schnittstellen-ID in einer IPv6-Adresse verwendet wird. Dazu geben Sie eine hexadezimale Zahl mit 64 Bit oder weniger ein, um die Schnittstellen-ID-Komponente der IPv6-Adresse zu belegen. Während der nachfolgenden automatischen Adresskonfiguration erstellt das Neighbor Discovery-Protokoll keine Schnittstellen-ID, die auf der MAC-Adresse der Schnittstelle basiert. Stattdessen wird das manuell erstellte Token zur Schnittstellen-ID. Das Token bleibt der Schnittstelle auch dann zugewiesen, wenn die Karte ausgetauscht wird.

Hinweis – Der Unterschied zwischen benutzerdefinierten Token und temporären Adressen besteht darin, dass temporäre Adressen zufällig erzeugt werden, während ein Token explizit von einem Benutzer erstellt wird.

▼ So konfigurieren Sie ein benutzerdefiniertes IPv6-Token

Die folgenden Anweisungen eignen sich insbesondere für Server, deren Schnittstellen regelmäßig ausgetauscht werden. Sie gelten auch für die Konfiguration von benutzerdefinierten Token auf einem IPv6-Knoten.

1 Prüfen Sie, ob die mit einem Token zu konfigurierende Schnittstelle geplumbt (aktiviert) wurde.

Eine Schnittstelle muss geplumbt sein, bevor Sie ein Token für ihre IPv6-Adresse konfigurieren können.

```
# ifconfig -a6

qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 0:3:ba:13:14:e1
        inet6 fe80::203:baff:fe13:14e1/10
```

Dieser Ausgabe zeigt, dass die Netzwerkschnittstelle `qfe0` geplumbt wurde und die Link-lokale Adresse `fe80::203:baff:fe13:14e1/10` aufweist. Diese Adresse wurde während der Konfiguration automatisch konfiguriert.

2 **Erstellen Sie eine oder mehrere hexadezimale Zahlen mit 64 Bit, die als Token für die Schnittstellen des Knoten verwendet werden. Beispiele für Token finden Sie unter** **„Link-lokale Unicast-Adresse“ auf Seite 83****.**

3 **Konfigurieren Sie jede Schnittstelle mit einem Token.**

Verwenden Sie die folgende Syntax des Befehls `ifconfig` für jede Schnittstelle, die eine benutzerdefinierte Schnittstellen-ID (Token) erhalten soll:

`ifconfig` *interface* `inet6  token` *address/64*

Verwenden Sie den folgenden Befehl, um die Schnittstelle `qfe0` mit einem Token zu konfigurieren:

```
# ifconfig qfe0 inet6 token ::1a:2b:3c:4d/64
```

Wiederholen Sie diesen Schritt für jede Schnittstelle, die ein benutzerdefiniertes Token erhalten soll.

4 **(Optional) Sorgen Sie dafür, dass die neue IPv6-Adresse auch nach einem Neustart beibehalten wird.**

a. **Erstellen oder bearbeiten Sie eine** `/etc/hostname6.`*Schnittstelle*-**Datei für jede Schnittstelle, die mit einem Token konfiguriert wurde.**

b. **Fügen Sie den folgenden Text am Ende jeder** `/etc/hostname6.`*Schnittstelle*-**Datei hinzu:**

`token ::`*token-name*`/64`

Sie können z. B. den folgenden Text am Ende einer `/etc/hostname6.`*Schnittstelle*-Datei hinzufügen:

```
token ::1a:2b:3c:4d/64
```

Nach dem Booten des Systems wird der Token, den Sie in der `/etc/hostname6.`*interface*-Datei konfiguriert haben, auf die IPv6-Adresse der Schnittstelle angewendet. Diese IPv6-Adresse bleibt auch bei nachfolgenden Neustarts bestehen.

5 **Aktualisieren Sie den IPv6-Daemon mit Ihren Änderungen.**

```
# pkill -HUP -in.ndpd
```

Beispiel 7–6 Konfiguration eines benutzerdefinierten Tokens auf einer IPv6-Schnittstelle

Im folgenden Beispiel weist die Schnittstelle `bge0:1` eine automatisch konfigurierte IPv6-Adresse auf. Das Teilnetzpräfix `2001:db8:3c4d:152:/64` wurde vom Router über den lokalen Link des Knotens bekannt gegeben. Die Schnittstellen-ID `2c0:9fff:fe56:8255` wurde aus `bge0:1`'s MAC-Adresse generiert.

```
# ifconfig -a6
lo0: flags=2002000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        inet6 ::1/128
bge0: flags=2100801 <UP,MULTICAST,IPv6> mtu 1500 index 5
        inet6 fe80::2c0:9fff:fe56:8255/10
        ether 0:c0:9f:56:82:55
bge0:1: flags=2180801 <UP, MULTICAST,ADDRCONF,IPv6>mtu 1500 index 5
        inet6 2001:db8:3c4d:152:c0:9fff:fe56:8255/64
# ifconfig bge0 inet6 token ::1a:2b:3c:4d/64
# vi /etc/hostname6.bge0
token ::1a:2b:3c:4d/64
# pkill -HUP -in.ndpd
# ifconfig -a6
lo0: flags=2002000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        inet6 ::1/128
bge0: flags=2100801 <UP,MULTICAST,IPv6> mtu 1500 index 5
        inet6 fe80::2c0:9fff:fe56:8255/10
        ether 0:c0:9f:56:82:55
bge0:1: flags=2180801 <UP, MULTICAST,ADDRCONF,IPv6>mtu 1500 index 5
        inet6 2001:db8:3c4d:152:1a:2b:3c:4d/64
```

Nachdem das Token konfiguriert wurde, führt die globale Adresse in der zweiten Statuszeile von `bge0:1` jetzt `1a:2b:3c:4d` als Konfiguration für dessen Schnittstellen-ID auf.

Siehe auch

- Informationen zum Aktualisieren des Namen-Services mit den IPv6-Adressen des Servers finden Sie unter „Konfiguration der Namen-Services-Unterstützung für IPv6“ auf Seite 213.
- Informationen zur Überwachung der Serverleistung finden Sie in Kapitel 8, „Verwaltung eines TCP/IP-Netzwerks (Aufgaben)“.

Verwaltung von IPv6-konformen Schnittstellen auf Servern

Wenn IPv6 auf einem Server eingesetzt werden soll, müssen Sie einige Entscheidungen treffen, bevor Sie IPv6 auf den Schnittstellen des Servers aktivieren. Ihre Entscheidungen wirken sich auf die Konfigurationsstrategie der Schnittstellen-IDs (bzw. *Token*) der IPv6-Adresse einer Schnittstelle aus.

▼ So aktivieren Sie IPv6 auf den Schnittstellen eines Servers

Bevor Sie beginnen

In dem nächsten Verfahren wird Folgendes vorausgesetzt:

- Oracle Solaris 10 ist bereits auf dem Server installiert.
- Sie haben IPv6 während der Installation von Oracle Solaris oder zu einem späteren Zeitpunkt gemäß den Angaben unter „Konfiguration einer IPv6-Schnittstelle" auf Seite 185 auf den Schnittstellen des Servers aktiviert.

Falls erforderlich, wurde die Anwendungssoftware zur Unterstützung von IPv6 aufgerüstet. Viele Anwendungen, die auf dem IPv4-Protokollstapel ausgeführt werden, unterstützen auch IPv6. Weitere Informationen hierzu finden Sie unter „So bereiten Sie Netzwerkservices auf die Unterstützung von IPv6 vor" auf Seite 95.

1. **Nehmen Sie auf dem Server die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Stellen Sie sicher, dass ein IPv6-Teilnetzpräfix auf einem Router auf dem gleichen Link wie der Server konfiguriert wurde.**

   Weitere Informationen hierzu finden Sie unter „Konfiguration eines IPv6-Routers" auf Seite 191.

3. **Verwenden Sie eine geeignete Strategie für die Schnittstellen-ID der IPv6-konformen Schnittstellen des Servers.**

   Standardmäßig verwendet die automatische IPv6-Adresskonfiguration die MAC-Adresse einer Schnittstelle zum Erstellen der Schnittstellen-ID-Komponente der IPv6-Adresse. Wenn die IPv6-Adresse der Schnittstelle bekannt ist, führt der Austausch einer Schnittstelle zu Problemen. Die MAC-Adresse der neuen Schnittstelle hat einen anderen Wert, somit wird bei der automatischen Adresskonfiguration eine neue Schnittstellen-ID erzeugt.

   - Bei einer IPv6-konformen Schnittstelle, die nicht ausgetauscht werden soll, verwenden Sie die automatisch konfigurierte IPv6-Adresse, die unter „Automatische IPv6-Adresskonfiguration" auf Seite 86 beschrieben wird.
   - Bei IPv6-konformen Schnittstellen, die außerhalb des lokalen Netzwerks anonym bleiben sollen, können Sie ein zufällig erzeugtes Token als Schnittstellen-ID verwenden. Anweisungen und Beispiele finden Sie unter „So konfigurieren Sie eine temporäre Adresse" auf Seite 197.

- Bei IPv6-konformen Schnittstellen, die regelmäßig ausgetauscht werden, erstellen Sie Token für die Schnittstellen-IDs. Anweisungen und Beispiele finden Sie unter „So konfigurieren Sie ein benutzerdefiniertes IPv6-Token“ auf Seite 200.

Aufgaben bei der Konfiguration von Tunneln zur Unterstützung von IPv6 (Übersicht der Schritte)

In der folgenden Tabelle sind die Aufgaben beschrieben, die zum Konfigurieren der verschiedenen IPv6-Tunnel erforderlich sind. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
Manuelle Konfiguration von IPv6-über-IPv4-Tunneln.	Erstellen Sie manuell einen IPv6-Tunnel über ein IPv4-Netzwerk, eine Lösung, um entfernte IPv6-Netzwerke innerhalb eines größeren, im Wesentlichen IPv4-konformen Unternehmensnetzwerk zu erreichen.	„So konfigurieren Sie einen IPv6-über-IPv4-Tunnel“ auf Seite 205
Manuelle Konfiguration von IPv6-über-IPv6-Tunneln.	Konfigurieren Sie manuell einen IPv6-Tunnel über ein IPv6-Netzwerk, das in der Regel innerhalb eines größeren Unternehmensnetzwerks verwendet wird.	„So konfigurieren Sie einen IPv6-über-IPv6-Tunnel“ auf Seite 206
Manuelle Konfiguration von IPv4-über-IPv6-Tunneln.	Konfigurieren Sie einen IPv4-Tunnel über ein IPv6-Netzwerk. Dies eignet sich insbesondere für große Netzwerke mit sowohl IPv4- als auch IPv6-Netzwerken.	„So konfigurieren Sie einen IPv4-über-IPv6-Tunnel“ auf Seite 207
Automatische Konfiguration von IPv6-über-IPv4-Tunneln (6to4-Tunnel).	Erstellen Sie einen automatischen 6to4-Tunnel, eine Lösung zum Erreichen eines externen IPv6-Standorts über das Internet.	„So konfigurieren Sie einen 6to4-Tunnel“ auf Seite 208
Konfiguration eines Tunnels zwischen einem 6to4-Router und einem 6to4-Relay-Router.	Aktivieren Sie mithilfe des `6to4relay`-Befehls einen Tunnel zu einem 6to4-Relay-Router.	„So konfigurieren Sie einen 6to4-Tunnel zu einem 6to4-Relay-Router“ auf Seite 211

Konfiguration von Tunneln zur Unterstützung von IPv6

IPv6-Netzwerke stellen in der großen IPv4-Welt häufig isolierte Entitäten dar. Knoten in Ihrem IPv6-Netzwerk müssen mit Knoten in isolierten IPv6-Netzwerken (innerhalb Ihres Unternehmens oder remote) kommunizieren können. In der Regel konfigurieren Sie einen Tunnel zwischen den IPv6-Routern, obwohl auch IPv6-Hosts als Endpunkte für Tunnel fungieren können. Informationen zur Tunnelplanung finden Sie unter „Planung für Tunnel in der Netzwerktopologie“ auf Seite 96.

Sie können automatisch oder manuell konfigurierte Tunnel für das IPv6-Netzwerk einrichten. Die Oracle Solaris IPv6-Implementierung unterstützt die folgenden Arten von Tunnel-Kapselungen:

- IPv6-über-IPv4-Tunnel
- IPv6-über-IPv6-Tunnel
- IPv4-über-IPv6-Tunnel
- 6to4-Tunnel

Konzeptuelle Beschreibungen der Tunnel finden Sie unter „IPv6-Tunnel“ auf Seite 308.

▼ So konfigurieren Sie einen IPv6-über-IPv4-Tunnel

In diesem Verfahren wird beschrieben, wie Sie einen Tunnel von einem IPv6-Knoten über ein IPv4-Netzwerk zu einem remoten IPv6-Knoten einrichten.

1. **Melden Sie sich beim lokalen Tunnelendpunkt als Primäradministrator oder als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Erstellen Sie die** `/etc/hostname6.ip.tun`*n***-Datei.**

   dabei steht *n* für die Tunnelnummer, beginnend mit null für den ersten Tunnel. Dann fügen Sie Einträge für die folgenden Unterschritte hinzu:

   a. **Fügen Sie die Ursprungsadresse des Tunnels und die Zieladresse hinzu.**

   `tsrc` *IPv4-source-address* `tdst` *IPv4-destination-address* `up`

   b. **(Optional) Fügen Sie eine logische Schnittstelle für die IPv6-Quell- und -Zieladresse hinzu.**

   `addif` *IPv6-source-address* *IPv6-destination-address*

   Lassen Sie diesen Unterschritt aus, wenn die Adresse für diese Schnittstelle automatisch konfiguriert werden soll. Sie müssen keine Link-lokalen Adressen für Ihren Tunnel konfigurieren.

3 **Starten Sie das System neu.**

4 **Wiederholen Sie diese Aufgabe am anderen Endpunkt des Tunnels.**

Beispiel 7–7 Eintrag in der `/etc/hostname6.ip.tun`-Datei für einen manuellen IPv6-über-IPv4-Tunnel

Diese `/etc/hostname6.ip.tun`-Beispieldatei zeigt einen Tunnel, für den globale Ursprungs- und Zieladressen manuell konfiguriert wurden.

```
tsrc 192.168.8.20 tdst 192.168.7.19 up
addif 2001:db8:3c4d:8::fe12:528 2001:db8:3c4d:7:a00:20ff:fe12:1234 up
```

▼ So konfigurieren Sie einen IPv6-über-IPv6-Tunnel

In diesem Verfahren wird beschrieben, wie Sie einen Tunnel von einem IPv6-Knoten über ein IPv6-Netzwerk zu einem remoten IPv6-Knoten einrichten

1 **Melden Sie sich beim lokalen Tunnelendpunkt als Primäradministrator oder als Superuser an.**

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 **Erstellen Sie die `/etc/hostname6.ip6.tun` *n*-Datei.**

Verwenden Sie für *n* die Werte 0, 1, 2 usw.. Dann fügen Sie Einträge für die folgenden Unterschritte hinzu.

a. **Fügen Sie die Ursprungsadresse des Tunnels und die Zieladresse hinzu.**

`tsrc` *IPv6-source-address* `tdst` *IPv6-destination-address*
IPv6-packet-source-address *IPv6-packet-destination-address* `up`

b. **(Optional) Fügen Sie eine logische Schnittstelle für die IPv6-Quell- und -Zieladresse hinzu.**

`addif` *IPv6-source-address* *IPv6-destination-address* `up`

Lassen Sie diesen Schritt aus, wenn die Adresse für diese Schnittstelle automatisch konfiguriert werden soll. Sie müssen keine Link-lokalen Adressen für Ihren Tunnel konfigurieren.

3 **Starten Sie das System neu.**

4 **Wiederholen Sie dieses Verfahren am anderen Endpunkt des Tunnels.**

Beispiel 7–8 Eintrag in der `/etc/hostname6.ip6.tun`-Datei für einen IPv6-über-IPv6-Tunnel

Das folgende Beispiel zeigt den Eintrag für einen IPv6-über-IPv6-Tunnel.

```
tsrc 2001:db8:3c4d:22:20ff:0:fe72:668c tdst 2001:db8:3c4d:103:a00:20ff:fe9b:a1c3
fe80::4 fe80::61 up
```

▼ So konfigurieren Sie einen IPv4-über-IPv6-Tunnel

In diesem Verfahren wird beschrieben, wie Sie einen Tunnel zwischen zwei IPv4-Hosts über ein IPv6-Netzwerk konfigurieren. Sie sollten dieses Verfahren anwenden, wenn das Netzwerk Ihrer Organisation heterogen ist und IPv6-Teilnetze enthält, die IPv4-Teilnetze voneinander trennen.

1. **Melden Sie sich beim lokalen IPv4-Tunnelendpunkt als Primäradministrator oder als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Erstellen Sie die** `/etc/hostname.ip6.tun`*n***-Datei.**

   Verwenden Sie für *n* die Werte 0, 1, 2 usw.. Dann fügen Sie Einträge für die folgenden Schritte hinzu:

   a. **Fügen Sie die Ursprungsadresse des Tunnels und die Zieladresse hinzu.**

      `tsrc` *IPv6-source-address* `tdst` *IPv6-destination-address*

   b. **(Optional) Fügen Sie für die IPv6-Quell- und -Zieladresse eine logische Schnittstelle hinzu.**

      `addif` *IPv6-source-address* *IPv6-destination-address* `up`

3. **Starten Sie den lokalen Host neu.**

4. **Wiederholen Sie dieses Verfahren am anderen Endpunkt des Tunnels.**

Beispiel 7–9 Eintrag in der `/etc/hostname6.ip6.tun`-Datei für einen IPv4-über-IPv6-Tunnel

Das folgende Beispiel zeigt den Eintrag für einen IPv4-über-IPv6-Tunnel.

```
tsrc 2001:db8:3c4d:114:a00:20ff:fe72:668c tdst 2001:db8:3c4d:103:a00:20ff:fe9b:a1c3
10.0.0.4 10.0.0.61 up
```

So konfigurieren Sie einen 6to4-Tunnel

Muss Ihr IPv6-Netzwerk mit einem remoten IPv6-Netzwerk kommunizieren können, sollten Sie die Verwendung von automatischen 6to4-Tunneln ein Betracht ziehen. Bei der Konfiguration eines 6to4-Tunnels muss der Grenzrouter als ein *6to4*-Router konfiguriert werden. Der 6to4-Router fungiert als Endpunkt eines 6to4-Tunnels zwischen Ihrem Netzwerk und einem Endpunkt-Router im remoten IPv6-Netzwerk.

Bevor Sie beginnen Bevor Sie das 6to4-Routing in einem IPv6-Netzwerk konfigurieren, müssen die folgenden Aufgaben abgeschlossen sein:

- Konfiguration von IPv6 auf allen entsprechenden Knoten am künftigen 6to4-Standort gemäß der Beschreibung unter „Modifizieren einer IPv6-Schnittstellenkonfiguration für Hosts und Server" auf Seite 196.
- Mindestens einen Router mit einer Verbindung zu einem IPv6-Netzwerk muss als 6to4-Router ausgewählt sein.
- Konfiguration einer global einmaligen IPv4-Adresse für die Schnittstelle des künftigen 6to4-Routers zum IPv4-Netzwerk. Die IPv4-Adresse muss statisch sein.

Hinweis – Verwenden Sie keine der in Kapitel 12, „Einführung in Oracle Solaris DHCP" beschriebenen dynamisch zugewiesenen IPv4-Adressen. Global dynamisch zugewiesene Adressen können sich mit der Zeit ändern, was sich negativ auf ihren IPv6-Adressierungsplan auswirkt.

---

1 Melden Sie sich auf dem künftigen 6to4-Router als Primäradministrator oder als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Konfigurieren Sie eine 6to4-Pseudoschnittstelle auf dem Router, indem Sie die `/etc/hostname6.ip.6to4tun0`-Datei erstellen.

- Wenn Sie beabsichtigen, die empfohlene Konvention von Teilnetz-ID=0 und Host-ID=1 beizubehalten, verwenden Sie das Kurzformat für `/etc/hostname6.ip.6to4tun0`:

  `tsrc` *IPv4-address* `up`

- Wenn Sie andere Konventionen für die Teilnetz-ID und Host-ID planen, verwenden Sie das Langformat für `/etc/hostname6.ip.6to4tun0`:

  `tsrc` *IPv4-address* `2002:`*IPv4-address*`:`*subnet-ID*`:`*interface-ID*`:/64 up`

Die erforderlichen Parameter für `/etc/hostname6.ip.6to4tun0` sind:

`tsrc` Gibt an, dass diese Schnittstelle als Tunnelquelle verwendet wird.

IPv4-Adresse — Gibt die im getrennten dezimalen Format auf der physikalischen Schnittstelle konfigurierte IPv4-Adresse an, die als 6to4-Pseudoschnittstelle verwendet werden soll.

Die übrigen Parameter sind optional. Wenn Sie jedoch einen der folgenden optionalen Parameter angeben, müssen Sie alle optionalen Parameter angeben.

`2002`	Gibt das 6to4-Präfix an.
IPv4-Adresse	Gibt die IPv4-Adresse der Pseudoschnittstelle in hexadezimaler Notation an.
Teilnetz-ID	Gibt eine andere Teilnetz-ID als 0 in hexadezimaler Notation an.
Schnittstellen-ID	Gibt eine andere Schnittstellen-ID als 1 an.
`/64`	Gibt an, dass das 6to4-Präfix eine Länge von 64 Bit aufweist.
`up`	Konfiguriert eine 6to4-Schnittstelle als “up.”

Hinweis – Zwei IPv6-Tunnel in Ihrem Netzwerk dürfen nicht die gleiche Ursprungs- und Zieladresse aufweisen, andernfalls werden Pakete abgeworfen. Dieses Szenario kann auftreten, wenn ein 6to4-Router nebenbei ein Tunneling über den `atun`-Befehl ausführt. Informationen zum `atun`-Befehl finden Sie in der Manpage `tun`(7M).

---

3 **(Optional) Erstellen Sie zusätzliche 6to4-Pseudoschnittstellen auf dem Router.**

Jede künftige 6to4-Pseudoschnittstelle muss über eine bereits konfigurierte, global einmalige IPv4-Adresse verfügen.

4 **Starten Sie den 6to4-Router neu.**

5 **Prüfen Sie den Status der Schnittstelle.**

```
# ifconfig ip.6to4tun0 inet6
```

Wenn die Schnittstelle korrekt konfiguriert wurde, erhalten Sie eine Ausgabe ähnlich der Folgenden:

```
ip.6to4tun0: flags=2200041<UP,RUNNING,NONUD,IPv6>mtu 1480 index 11
        inet tunnel src 111.222.33.44
        tunnel hop limit 60
        inet6 2002:6fde:212c:10:/64
```

6 **Bearbeiten Sie die `/etc/inet/ndpd.conf`-Datei, um das 6to4-Routing bekannt zu geben.**

Ausführliche Informationen finden Sie in der Manpage `ndpd.conf(4)`.

a. **Geben Sie das Teilnetz an, das die Advertisement-Nachrichten zuerst empfangen soll.**

Erstellen Sie einen `if`-Eintrag im folgenden Format:

`if` *subnet-interface* `AdvSendAdvertisements 1`

Um das 6to4-Routing beispielsweise in dem mit der Schnittstelle `hme0` verbundenen Teilnetz bekannt zu geben, ersetzen Sie *Teilnetzschnittstelle* durch `hme0`.

```
if hme0 AdvSendAdvertisements 1
```

b. **Fügen Sie das 6to4-Präfix der Advertisement-Nachrichten als zweite Zeile hinzu.**

Erstellen Sie einen `prefix`-Eintrag im folgenden Format:

`prefix 2002:`*IPv4-address*`:`*subnet-ID*`::/64` *subnet-interface*

7 **Starten Sie den Router neu.**

Alternativ können Sie ein `sighup` an den `/etc/inet/in.ndpd`-Daemon ausgeben, um das Senden der Router-Advertisement-Nachrichten zu beginnen. Die IPv6-Knoten in jedem Teilnetz, das das 6to4-Präfix empfängt, beginnen mit der automatischen Konfiguration der neuen 6to4-abgeleiteten Adressen.

8 **Fügen Sie die neuen 6to4-abgeleiteten Adressen der Knoten zu dem Namen-Service hinzu, der an dem 6to4-Standort verwendet wird.**

Anweisungen finden Sie unter „Konfiguration der Namen-Services-Unterstützung für IPv6“ auf Seite 213.

Beispiel 7–10 6to4-Routerkonfiguration (Kurzform)

Das Folgende ist ein Beispiel der Kurzform von `/etc/hostname6.ip.6to4tun0`:

```
# cat /etc/hostname6.ip.6to4tun0
tsrc 111.222.33.44 up
```

Beispiel 7–11 6to4-Routerkonfiguration (Langform)

Das Folgende ist ein Beispiel der Langform von `/etc/hostname6.ip.6to4tun0`:

```
# cat /etc/hostname6.ip.6to4tun0
tsrc 111.222.33.44 2002:6fde:212c:20:1/64 up
```

Beispiel 7–12 `ifconfig`-Ausgabe zeigt 6to4-Pseudoschnittstelle

Das folgende Beispiel zeigt die Ausgabe des `ifconfig`-Befehls für eine 6to4-Pseudoschnittstelle:

```
# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NONUD,IPv6> mtu 1480 index 11
        inet tunnel src 192.168.87.188
        tunnel hop limit 60
        inet6 2002:c0a8:57bc::1/64
```

Beispiel 7–13 6to4-Advertisement-Nachrichten in `/etc/inet/ndpd.conf`

Die folgende `/etc/inet/ndpd.conf`-Beispieldatei gibt das 6to4-Routing in zwei Teilnetzen bekannt:

```
if qfe0 AdvSendAdvertisements 1
prefix  2002:c0a8:57bc:10::/64 qfe0

if qfe1 AdvSendAdvertisements 1
prefix  2002:c0a8:57bc:2::/64 qfe1
```

Weitere Informationen: Konfiguration von mehreren Routern am 6to4-Standort

Bei einem Standort mit mehreren Routern müssen die Router hinter dem 6to4-Router für die Unterstützung von 6to4 konfiguriert werden. Wenn an Ihrem Standort RIP verwendet wird, müssen Sie die statischen Routen zum 6to4-Router auf jedem nicht-6to4-Router konfigurieren. Wenn Sie ein kommerzielles Routing-Protokoll verwenden, müssen Sie keine statischen Routen zum 6to4-Router erstellen.

▼ So konfigurieren Sie einen 6to4-Tunnel zu einem 6to4-Relay-Router

Achtung – Aufgrund schwerwiegender Sicherheitsprobleme ist die Unterstützung von 6to4-Relay-Routern in Oracle Solaris standardmäßig deaktiviert. Lesen Sie dazu „Sicherheitsbetrachtungen beim Tunneling zu einem 6to4-Relay-Router“ auf Seite 250.

Bevor Sie beginnen Bevor Sie einen Tunnel zu einem 6to4-Relay-Router aktivieren, müssen die folgenden Aufgaben vollständig abgeschlossen sein:

- Konfiguration eines 6to4-Routers an Ihrem Standort gemäß der Beschreibung unter „So konfigurieren Sie einen 6to4-Tunnel“ auf Seite 208
- Prüfung aller Sicherheitspunkte beim Tunneling zu einem 6to4-Relay-Router

1 Melden Sie sich auf dem 6to4-Router als Primäradministrator oder als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Aktivieren Sie einen Tunnel zu einem 6to4-Relay-Router, indem Sie eines der folgenden Formate verwenden:

- Aktivieren Sie einen Tunnel zu einem Anycast-6to4-Relay-Router.

  ```
  # /usr/sbin/6to4relay -e
  ```

  Die Option `-e` stellt einen Tunnel zwischen dem 6to4-Router und einem Anycast-6to4-Relay-Router her. Anycast-6to4-Relay-Router haben die bekannte IPv4-Adresse `192.88.99.1`. Der Anycast-Relay-Router, der Ihrem Standort am nächsten ist, wird zum Endpunkt für den 6to4-Tunnel. Dieser Relay-Router wickelt dann die Paketweiterleitung zwischen Ihrem 6to4-Standort und einem nativen IPv6-Standort ab.

  Ausführliche Informationen zu Anycast-6to4-Relay-Routern finden Sie in RFC 3068, „An Anycast Prefix for 6to4 Relay Routers" (`ftp://ftp.rfc-editor.org/in-notes/rfc3068.txt`).

- Aktivieren Sie einen Tunnel zum angegebenen 6to4-Relay-Router.

  ```
  # /usr/sbin/6to4relay -e -a relay-router-address
  ```

  Die Option `-a` gibt an, dass einer bestimmten Routeradresse gefolgt werden muss. Ersetzen Sie *Relay-Router-Adresse* durch die IPv4-Adresse des 6to4-Relay-Routers, zu dem Sie einen Tunnel einrichten möchten.

Der Tunnel zum 6to4-Relay-Router bleibt aktiv, bis Sie die 6to4-Pseudoschnittstelle des Tunnels entfernen.

3 Löschen Sie dem Tunnel zum 6to4-Relay-Router, wenn er nicht mehr benötigt wird:

```
# /usr/sbin/6to4relay -d
```

4 (Optional) Sorgen Sie dafür, dass der Tunnel zum 6to4-Relay-Router auch nach einem Neustart beibehalten wird.

An Ihrem Standort kann es einen zwingenden Grund geben, warum der Tunnel zum 6to4-Relay-Router nach jedem Neustart des 6to4-Routers wiederhergestellt werden soll. Für dieses Szenario müssen Sie Folgendes ausführen:

a. Bearbeiten Sie die `/etc/default/inetinit`-Datei.

Die zu ändernde Zeile befindet sich am Ende der Datei.

b. Ändern Sie den Wert „NO" in der Zeile `ACCEPT6TO4RELAY=NO` zu „YES".

c. (Optional) Erstellen Sie einen Tunnel zu einem bestimmten 6to4-Relay-Router, der auch nach einem Neustart beibehalten wird.

Für den Parameter `RELAY6TO4ADDR` ändern Sie die Adresse `192.88.99.1` in die IPv4-Adresse des zu verwendenden 6to4-Relay-Routers.

Beispiel 7–14 Abrufen von Statusinformationen zur Unterstützung von 6to4-Relay-Routern

Mit dem Befehl `/usr/bin/6to4relay` können Sie prüfen, ob die Unterstützung für 6to4-Relay-Router aktiviert wurde. Das nächste Beispiel zeigt die Ausgabe, wenn die Unterstützung für 6to4-Relay-Router deaktiviert wurde (dies ist die Standardeinstellung in Oracle Solaris):

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is disabled.
```

Wenn die Unterstützung für 6to4-Relay-Router aktiviert wurde, erhalten Sie die folgende Ausgabe:

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is enabled.
IPv4 remote address of Relay Router=192.88.99.1
```

Konfiguration der Namen-Services-Unterstützung für IPv6

In diesem Abschnitt wird beschrieben, wie die Namen-Services DNS und NIS so konfigurieren, dass sie die IPv6-Services unterstützen.

Hinweis – LDAP unterstützt IPv6, ohne dass IPv6-spezifische Konfigurationsschritte durchgeführt werden müssen.

Umfassende Informationen zur Verwaltung von DNS, NIS und LDAP finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

▼ So fügen Sie IPv6-Adressen zum DNS hinzu

1. **Melden Sie sich als Primäradministrator oder als Superuser beim primären oder sekundären DNS-Server an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Bearbeiten Sie die entsprechende DNS-Zone-Datei, indem Sie AAAA-Einträge für jeden IPv6-konformen Knoten hinzufügen:**

   host-name `IN AAAA` *host-address*

3. **Bearbeiten Sie die DNS-Reverse Zone-Datei und fügen Sie PTR-Datensätze hinzu:**

   host-address `IN PTR` *hostname*

   Ausführliche Informationen zur DNS-Verwaltung finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

Beispiel 7–15 DNS-Reverse Zone-Datei

Das folgende Beispiel zeigt eine IPv6-Adresse in der Reverse Zone-Datei.

```
$ORIGIN    ip6.int.
8.2.5.0.2.1.e.f.f.f.9.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.0.0.2.0.0.0 \
    IN        PTR        vallejo.Eng.apex.COM.
```

Hinzufügen von IPv6-Adressen zum NIS

In Solaris 10 11/06 und früheren Releases wurden zwei Maps (Zuordnungslisten) für NIS hinzugefügt: `ipnodes.byname` und `ipnodes.byaddr`. Diese Maps enthalten sowohl IPv4- als auch IPv6-Hostnamen sowie Adresszuweisungen. Tools, die IPv6 unterstützen, verwenden die NIS-Maps `ipnodes.` Die Maps `hosts.byname` und `hosts.byaddr` enthalten nur den IPv4-Hostnamen sowie Adresszuweisungen. Diese Maps bleiben unverändert, so dass sie das Arbeiten mit vorhandenen Anwendungen vereinfachen können. Die Verwaltung der `ipnodes`-Maps verläuft ähnlich der Verwaltung der Maps `hosts.byname` und `hosts.byaddr.` Unter Solaris 10 11/06 ist es wichtig, dass Sie die *hosts*-Maps mit den IPv4-Adressen aktualisieren, die *ipnode*-Maps werden ebenfalls mit den gleichen Informationen aktualisiert.

Hinweis – Nachfolgende Versionen von Oracle Solaris 10 werden die `ipnodes`-Maps nicht mehr verwenden. Die IPv6-Funktionalität der `ipnodes`-Maps wird jetzt in den `hosts`-Maps verwaltet.

Anweisungen zur Verwaltung der NIS-Maps finden Sie in Kapitel 5, „Setting Up and Configuring NIS Service" in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

▼ So zeigen Sie Informationen zum IPv6-Namen-Service an

Mit dem Befehl `nslookup` können Sie Informationen zum IPv6-Namen-Service anzeigen.

1. **Führen Sie den Befehl `nslookup` von Ihrem Benutzerkonto aus.**

```
% /usr/sbin/nslookup
```

Es werden der standardmäßige Servername und die -adresse angezeigt, gefolgt von der Eingabeaufforderung des `nslookup`-Befehls.

2. **Zeigen Sie Informationen zu einem bestimmten Host an, indem Sie die folgenden Befehle an der Eingabeaufforderung eingeben:**

```
>set q=any
>host-name
```

3. **Geben Sie den folgenden Befehl ein, um nur die AAAA-Datensätze anzuzeigen:**

```
>set q=AAAA
hostname
```

4. **Beenden Sie den `nslookup`-Befehl durch Eingabe von `exit`.**

Beispiel 7–16 Verwenden von `nslookup` zur Anzeige von IPv6-Informationen

Das folgende Beispiel zeigt die Ergebnisse des `nslookup`-Befehls in einer IPv6-Netzwerkumgebung.

```
%  /usr/sbin/nslookup
Default Server:  dnsserve.local.com
Address:  10.10.50.85
> set q=AAAA
> host85
Server:  dnsserve.local.com
Address:  10.10.50.85
```

```
host85.local.com      IPv6 address = 2::9256:a00:fe12:528
> exit
```

So prüfen Sie, ob die DNS IPv6 PTR-Datensätze korrekt aktualisiert wurden

In diesem Verfahren verwenden Sie den `nslookup`-Befehl zur Anzeige der PTR-Datensätze für DNS IPv6.

1. **Führen Sie den Befehl `nslookup` von Ihrem Benutzerkonto aus.**

   ```
   % /usr/sbin/nslookup
   ```

   Es werden der standardmäßige Servername und die -adresse angezeigt, gefolgt von der Eingabeaufforderung des `nslookup`-Befehls.

2. **Geben Sie Folgendes an der Eingabeaufforderung ein, um die PTR-Datensätze anzuzeigen:**

   ```
   >set q=PTR
   ```

3. **Beenden Sie den Befehl durch Eingabe von `exit`.**

Beispiel 7–17 Verwenden von `nslookup` zur Anzeige von PTR-Datensätzen

Im folgenden Beispiel wird gezeigt, wie die PTR-Datensätze mit dem Befehl `nslookup` angezeigt werden.

```
%  /usr/sbin/nslookup
Default Server:  space1999.Eng.apex.COM
Address:  192.168.15.78
> set q=PTR
> 8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.0.0.2.0.0.0.ip6.int

8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.0.0.2.0.0.0.ip6.int name =
vallejo.ipv6.Eng.apex.COM
ip6.int nameserver = space1999.Eng.apex.COM
> exit
```

So zeigen Sie IPv6-Informationen über NIS an

In diesem Verfahren verwenden Sie den Befehl `ypmatch`, um IPv6-Informationen über NIS anzuzeigen:

- **Geben Sie von Ihrem Benutzerkonto aus den folgenden Befehl ein, um die IPv6-Adressen in NIS anzuzeigen:**

  % **ypmatch** *hostname* **hosts ipnodes.***byname*

Es werden Informationen über den angegebenen *Hostnamen* angezeigt.

Hinweis – Oracle Solaris-Versionen nach Solaris 11/06 enthalten keine `ipnodes`-Maps. Die IPv6-Funktionalität von `ipnodes` wird jetzt von den `hosts`-Maps verwaltet.

Beispiel 7–18 IPv6-Adressenausgabe durch den Befehl `ypmatch`

Unter Solaris 10 11/06 und früheren Releases zeigt das folgende Beispiel die Ergebnisse eines `ypmatch`-Vorgangs an der `ipnodes.byname`-Datenbank an.

```
% ypmatch farhost hosts ipnodes.byname
2001:0db8:3c4d:15:a00:20ff:fe12:5286       farhost
```

So zeigen Sie IPv6-Informationen unabhängig vom Namen-Service an

Das folgende Verfahren kann nur unter Solaris 10 11/06 und früheren Releases angewendet werden. Unter nachfolgenden Releases können Sie den gleichen Vorgang an der `hosts`-Datenbank vornehmen.

- **Geben Sie von Ihrem Benutzerkonto aus den folgenden Befehl ein:**

  % **getent ipnodes** *hostname*

  Es werden Informationen über den angegebenen *Hostnamen* angezeigt.

Beispiel 7–19 Anzeigen von IPv6-Informationen in der `ipnodes`-Datenbank

Im folgenden Beispiel wird die Ausgabe des `getent`-Befehls angezeigt:

```
% getent ipnodes vallejo

2001:0db8:8512:2:56:a00:fe87:9aba    myhost myhost
fe80::56:a00:fe87:9aba     myhost myhost
```

KAPITEL 8

Verwaltung eines TCP/IP-Netzwerks (Aufgaben)

In diesem Kapitel werden die Aufgaben zur Verwaltung eines TCP/IP-Netzwerks beschrieben. Es umfasst die folgenden Themen:

- „Aufgaben bei der Verwaltung von TCP/IP Netzwerken (Übersicht der Schritte)" auf Seite 220
- „Überwachen der Schnittstellenkonfiguration mit dem Befehl `ifconfig`" auf Seite 221
- „Überwachen des Netzwerkstatus mit dem Befehl `netstat`" auf Seite 225
- „Ermitteln des Status von Remote-Hosts mit dem Befehl `ping`" auf Seite 232
- „Verwalten und Protokollieren der Netzwerkstatusanzeigen" auf Seite 234
- „Anzeigen von Routing-Informationen mit dem Befehl `traceroute`" auf Seite 237
- „Überwachen der Paketübertragungen mit dem Befehl `snoop`" auf Seite 238
- „Verwaltuen der standardmäßigen Adressauswahl" auf Seite 242

Bei den folgenden Aufgaben wird davon ausgegangen, dass ein betriebsfähiges TCP/IP-Netzwerk an Ihrem Standort installiert ist, das entweder nur IPv4 oder den Dual-Stack IPv4/IPv6 unterstützt. Wenn IPv6 an Ihrem Standort implementiert werden soll, dies aber noch nicht erfolgt ist, lesen Sie zunächst die folgenden Kapitel:

- Informationen zur Planung einer IPv6-Implementierung in Kapitel 4, „Planen eines IPv6-Netzwerks (Aufgaben)".
- Informationen zur Konfiguration von IPv6 und zum Erstellen einer Dual-Stack-Netzwerkumgebung finden Sie in Kapitel 7, „Konfigurieren eines IPv6-Netzwerks (Vorgehen)".

Aufgaben bei der Verwaltung von TCP/IP Netzwerken (Übersicht der Schritte)

In der folgenden Tabelle werden weitere Aufgaben zur Netzwerkverwaltung nach der anfänglichen Konfiguration aufgeführt, wie beispielsweise das Anzeigen von Netzwerkinformationen. Die Tabelle enthält Beschreibungen des Zwecks der einzelnen sowie die Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Weitere Informationen
Anzeigen der Konfigurationsinformationen einer Schnittstelle.	Ermitteln Sie die aktuelle Konfiguration jeder Schnittstelle auf einem System.	„So zeigen Sie Informationen zu einer bestimmten Schnittstelle an" auf Seite 221
Anzeigen der Schnittstellen-Adresszuweisungen.	Ermitteln Sie die Adresszuweisungen für alle Schnittstellen auf dem lokalen System.	„So zeigen Sie die Schnittstellen-Adresszuweisungen an" auf Seite 223
Anzeigen der Statistiken auf Protokollbasis.	Zeigen Sie die Leistung der Netzwerkprotokolle eines bestimmten Systems an.	„So zeigen Sie Statistiken nach dem Protokoll an" auf Seite 226
Anzeigen des Netzwerkstatus.	Überwachen Sie Ihr System, indem Sie alle Socket- und Routing-Tabellen-Einträge anzeigen. Die Ausgabe umfasst die inet-Adressfamilie für IPv4 und die inet6-Adressfamilie für IPv6.	„So zeigen Sie den Status der Sockets an" auf Seite 229
Anzeigen des Status der Netzwerkschnittstellen.	Überwachen Sie die Leistung der Netzwerkschnittstellen. Dies eignet sich insbesondere für die Behebung von Übertragungsproblemen.	„So zeigen Sie den Netzwerkschnittstellenstatus an" auf Seite 228
Anzeigen des Paket-Übertragungsstatus.	Überwachen Sie den Status der Pakete, während sie über das Netzwerk gesendet werden.	„So zeigen Sie den Status von Paketübertragungen eines bestimmten Adresstyps an" auf Seite 230
Steuern der Ausgabe von IPv6-bezogenen Befehlen.	Steuern Sie die Ausgabe der Befehle `ping`, `netstat`, `ifconfig` und `traceroute`. Erstellen Sie eine Datei mit dem Namen `inet_type`. Richten Sie die Variable `DEFAULT_IP` in dieser Datei ein.	„So steuern Sie die Anzeige der Ausgabe von IP-bezogenen Befehlen" auf Seite 234

Aufgabe	Beschreibung	Weitere Informationen
Überwachen des Netzwerkverkehrs.	Zeigen Sie alle IP-Pakete mit dem Befehl snoop an.	„So überwachen Sie den IPv6-Netzwerkverkehr" auf Seite 241
Verfolgen aller Routen, die dem Netzwerk-Routern bekannt sind.	Verwenden Sie den Befehl traceroute, um alle Routen anzuzeigen.	„So verfolgen Sie alle Routen" auf Seite 238

Überwachen der Schnittstellenkonfiguration mit dem Befehl ifconfig

Mit dem Befehl ifconfig können Sie Schnittstellen manuell IP-Adressen zuweisen und die Schnittstellenparameter manuell konfigurieren. Darüber hinaus führen die Oracle Solaris-Startskripten ifconfig aus, um Pseudoschnittstellen wie z. B. 6to4-Tunnelendpunkte zu konfigurieren.

Dieses Buch enthält zahlreiche Aufgaben, die verschiedene Optionen des vielseitigen Befehls ifconfig nutzen. Eine vollständige Beschreibung dieses Befehls, seiner Optionen und der Variablen finden Sie in der Manpage ifconfig(1M) Die allgemeine Syntax des Befehls ifconfig lautet:

ifconfig *Schnittstelle [Protokollfamilie]*

▼ So zeigen Sie Informationen zu einer bestimmten Schnittstelle an

Mit dem Befehl ifconfig können Sie allgemeine Informationen zu den Schnittstellen eines bestimmten Systems ermitteln. Beispielsweise kann eine einfache ifconfig -Abfrage folgende Informationen liefern:

- Die Gerätenamen aller Schnittstellen eines Systems
- Alle IPv4- und, sofern anwendbar, alle IPv6-Adressen, die den Schnittstellen zugewiesen wurden
- Welche Schnittstellen derzeit konfiguriert sind

Im folgenden Verfahren wird gezeigt, wie Sie den Befehl ifconfig verwenden, um allgemeine Konfigurationsinformationen zu den Schnittstellen eines Systems zu beziehen.

1. **Nehmen Sie auf dem lokalen Host die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Rufen Sie die Informationen einer bestimmten Schnittstelle ab.**

   `# ifconfig` *interface*

   Die Ausgabe des ifconfig-Befehls hat das folgende Format:

   - Statuszeile

     Die erste Zeile der Ausgabe des `ifconfig`-Befehls enthält den Schnittstellennamen sowie die Status-Flags, die der Schnittstelle derzeit zugeordnet sind. Darüber hinaus enthält die Statuszeile die Höchstzahl an Übertragungseinheiten (Maximum Transmission Unit, MTU), die für die Schnittstelle konfiguriert wurde, sowie eine Indexnummer. Anhand der Statuszeile stellen Sie den aktuellen Status der Schnittstelle fest.

   - Informationszeile mit der IP-Adresse

     Die zweite Zeile der Ausgabe des `ifconfig`-Befehls enthält die IPv4- oder die IPv6-Adresse, die für die Schnittstelle konfiguriert wurde. Bei einer IPv4-Adresse werden darüber hinaus die konfigurierte Netzmaske und die Broadcast-Adresse angezeigt.

   - MAC-Adresszeile

     Wenn Sie den Befehl `ifconfig` als Superuser oder in einer ähnlichen Rolle ausführen, enthält die Ausgabe des Befehls `ifconfig` eine dritte Zeile. Bei einer IPv4-Adresse finden Sie hier die der Schnittstelle zugewiesene MAC-Adresse (Ethernet-Schicht-Adresse). Bei einer IPv6-Adresse wird in der dritten Zeile die Link-lokale Adresse angezeigt, die der `in.ndpd`-Daemon aus der MAC-Adresse erzeugt hat.

Beispiel 8–1 Allgemeine Schnittstelleninformationen des Befehls `ifconfig`

Das folgende Beispiel zeigt, wie Sie mithilfe des Befehls `ifconfig` Informationen zur Schnittstelle `eri` auf einem bestimmten Host beziehen.

```
# ifconfig eri
eri0: flags=863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 1
      inet 10.0.0.112 netmask ffffff80 broadcast 10.8.48.127
      ether 8:0:20:b9:4c:54
```

In der folgenden Tabelle werden die Variableninformationen in einer `ifconfig`-Abfrage beschrieben, sowie wie die Variable auf dem Bildschirm angezeigt werden kann und welche Informationen bereitgestellt werden. Als Beispiel wird die vorherige Ausgabe verwendet.

Variable	Bildschirmausgabe	Beschreibung
Schnittstellen-name	eri0	Gibt den Gerätenamen der Schnittstelle an, deren Status mit dem Befehl ifconfig angefordert wurde.
Schnittstellen-status	flags=863<UP	Zeigt den Status der Schnittstelle an, einschließlich aller Flags, die der Schnittstelle derzeit zugeordnet sind. Hier können Sie feststellen, ob die Schnittstelle momentan initialisiert ist (UP) oder nicht (DOWN).
Broadcaststatus	BROADCAST	Gibt an, ob die Schnittstelle IPv4-Broadcasts unterstützt.
Übertragungs-status	RUNNING	Gibt an, ob das System derzeit Pakete über die Schnittstelle überträgt.
Multicaststatus	MULTICAST, IPv4	Zeigt an, ob die Schnittstelle Multicast-Übertragungen unterstützt. Die Beispielschnittstelle unterstützt IPv4-Multicast-Übertragungen.
Maximale Übertragungs-einheit	mtu 1500	Zeigt an, das diese Schnittstelle über eine maximale Übertragungsgröße von 1500 Oktetts verfügt.
IP-Adresse	inet 10.0.0.112	Zeigt die der Schnittstelle zugewiesene IPv4- oder IPv6-Adresse an. Die Beispielschnittstelle eri0 hat die IPv4-Adresse 10.0.0.112 .
Netzmaske	netmask ffffff80	Zeigt die IPv4-Netzmaske der betreffenden Schnittstelle an. Beachten Sie, dass IPv6-Adressen keine Netzmasken verwenden.
MAC-Adresse	ether 8:0:20:b9:4c:54	Zeigt die Ethernet-Schicht-Adresse der Schnittstelle an.

▼ So zeigen Sie die Schnittstellen-Adresszuweisungen an

Router und Multihomed-Hosts verfügen über mehrere Schnittstellen, häufig sind jeder Schnittstelle sogar mehrere IP-Adressen zugewiesen. Mit dem Befehl `ifconfig` können Sie alle Adressen anzeigen, die den Schnittstellen eines Systems zugewiesen sind. Darüber hinaus können Sie mit dem Befehl `ifconfig` auch ausschließlich die IPv4- oder die IPv6-Adresszuweisungen anzeigen. Um zusätzlich die MAC-Adressen der Schnittstellen anzuzeigen, müssen Sie sich entweder als Superuser angemeldet oder eine entsprechende Rolle angenommen haben.

Weitere Informationen zum Befehl `ifconfig` finden Sie in der Manpage `ifconfig`(1M).

1 Nehmen Sie auf dem lokalen System die Rolle eines Netzwerkmanagers an, oder melden Sie sich als Superuser an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2 Zeigen Sie die Informationen zu allen Schnittstellen an.

Sie können auch Variationen des Befehls `ifconfig -a` verwenden, um Folgendes auszuführen:

- Anzeigen aller Adressen aller Schnittstellen eines Systems.

```
# ifconfig -a
```

- Anzeigen aller IPv4-Adressen, die den Schnittstellen eines Systems zugewiesen sind.

```
# ifconfig -a4
```

- Wenn das lokale System IPv6-konform ist, Anzeigen aller IPv6-Adressen, die den Schnittstellen eines Systems zugewiesen sind.

```
ifconfig -a6
```

Beispiel 8–2 Anzeigen der Adressinformationen aller Schnittstellen

In diesem Beispiel werden die Einträge eines Hosts gezeigt, der nur über eine primäre Netzwerkschnittstelle, `qfe0`, verfügt. Dennoch zeigt die Ausgabe des Befehls `ifconfig`, dass `qfe0` derzeit drei Adressformen zugewiesen sind: Loopback (`lo0`), IPv4 (`inet`) und IPv6 (`inet6`). Im IPv6-Abschnitt der Ausgabe enthält eine Zeile für die Schnittstelle `qfe0` die Link-lokale IPv6-Adresse. Die zweite Adresse für `qfe0` wird in der Zeile `qfe0:1` angezeigt.

```
% ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
qfe0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.112 netmask ffffff80 broadcast 10.0.0.127
        ether 8:0:20:b9:4c:54
lo0: flags=2000849 <UP,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 8:0:20:b9:4c:54
        inet6 fe80::a00:20ff:feb9:4c54/10
qfe0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
        inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64
```

Beispiel 8–3 Anzeigen der Adressinformationen aller IPv4-Schnittstellen

Das folgende Beispiel zeigt die IPv4-Adresse, die für einen Multihomed-Host konfiguriert wurde. Um diese Form des `ifconfig`-Befehls auszuführen, müssen Sie nicht als Superuser angemeldet sein.

```
% ifconfig -a4
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
qfe0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.112 netmask ffffff80 broadcast 10.0.0.127
        ether 8:0:20:b9:4c:54
qfe1: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.118 netmask ffffff80 broadcast 10.0.0.127
        ether 8:0:20:6f:5e:17
```

Beispiel 8–4 Anzeigen der Adressinformationen aller IPv6-Schnittstellen

In diesem Beispiel wird gezeigt nur die IPv6-Adressen, die für einen bestimmten Host konfiguriert wurden. Um diese Form des `ifconfig`-Befehls auszuführen, müssen Sie nicht als Superuser angemeldet sein.

```
% ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 8:0:20:b9:4c:54
        inet6 fe80::a00:20ff:feb9:4c54/10
qfe0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
        inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64
```

Diese Ausgabe des Befehls `ifconfig` zeigt die folgenden drei Arten von IPv6-Adressformen, die einer einzelnen Schnittstelle eines Hosts zugewiesen sind:

`lo0`
IPv6-Loopback-Adresse.

`inet6 fe80::a00:20ff:feb9:4c54/10`
Link-lokale Adresse, die der primären Netzwerkschnittstelle zugewiesen wurde.

`inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64`
IPv6-Adresse, einschließlich Teilnetzpräfix. Der Begriff `ADDRCONF` in der Ausgabe deutet darauf hin, dass diese Adresse automatisch vom Host konfiguriert wurde.

Überwachen des Netzwerkstatus mit dem Befehl `netstat`

Der Befehl `netstat` erzeugt eine Anzeige, in der Netzwerkstatus und Protokollstatistiken aufgeführt werden. Sie können den Status von TCP-, SCTP- und UDP-Endpunkten in einem Tabellenformat anzeigen. Darüber hinaus können Sie Routing-Tabelleninformationen sowie Schnittstelleninformationen anzeigen.

Der Befehl `netstat` zeigt, abhängig von der gewählten Befehlszeilenoption, verschiedene Arten von Netzwerkdaten an. Diese Anzeigen eignen sich besonders für die Systemverwaltung. Die allgemeine Syntax für den Befehl `netstat` lautet:

`netstat` [`-m`] [`-n`] [`-s`] [`-i` | `-r`] [`-f` *Adressfamilie*]

In diesem Abschnitt werden die am häufigsten verwendeten Optionen des Befehls `netstat` beschrieben. Eine ausführliche Beschreibung aller `netstat`-Optionen finden Sie in der Manpage `netstat`(1M).

So zeigen Sie Statistiken nach dem Protokoll an

Mit der Option `netstat -s` zeigen Sie Protokollstatistiken für die Protokolle UDP, TCP, SCTP, ICMP und IP an.

Hinweis – Zum Anzeigen der Ausgabe des `netstat`-Befehls können Sie Ihr Oracle Solaris-Benutzerkonto verwenden.

- **Zeigen Sie den Protokollstatus an.**

```
$ netstat -s
```

Beispiel 8–5 Netzwerkprotokollstatistiken

Das folgende Beispiel zeigt die Ausgabe des Befehls `netstat - s` an. Die Ausgabe wurde teilweise verkürzt. Die Ausgabe kann Bereiche enthalten, in denen ein Problem bei einem Protokoll auftritt. Beispielsweise können statistische Informationen von ICMPv4 und ICMPv6 darauf hindeuten, wo das ICMP-Protokoll Fehler gefunden hat.

```
RAWIP
        rawipInDatagrams    =  4701     rawipInErrors       =     0
        rawipInCksumErrs    =     0     rawipOutDatagrams   =     4
        rawipOutErrors      =     0

UDP
        udpInDatagrams      = 10091     udpInErrors         =     0
        udpOutDatagrams     = 15772     udpOutErrors        =     0

TCP     tcpRtoAlgorithm     =     4     tcpRtoMin           =   400
        tcpRtoMax           = 60000     tcpMaxConn          =    -1
        .
        .
        tcpListenDrop       =     0     tcpListenDropQ0     =     0
        tcpHalfOpenDrop     =     0     tcpOutSackRetrans   =     0

IPv4    ipForwarding        =     2     ipDefaultTTL        =   255
        ipInReceives        =300182     ipInHdrErrors       =     0
        ipInAddrErrors      =     0     ipInCksumErrs       =     0
        .
        .
        ipsecInFailed       =     0     ipInIPv6            =     0
        ipOutIPv6           =     3     ipOutSwitchIPv6     =     0

IPv6    ipv6Forwarding      =     2     ipv6DefaultHopLimit =   255
        ipv6InReceives      = 13986     ipv6InHdrErrors     =     0
        ipv6InTooBigErrors  =     0     ipv6InNoRoutes      =     0
        .
        .
        rawipInOverflows    =     0     ipv6InIPv4          =     0

       ipv6OutIPv4         =     0     ipv6OutSwitchIPv4   =     0
```

```
ICMPv4  icmpInMsgs          = 43593     icmpInErrors        =     0
        icmpInCksumErrs     =     0     icmpInUnknowns      =     0
        .
        .
        icmpInOverflows     =     0

ICMPv6  icmp6InMsgs         = 13612     icmp6InErrors       =     0
        icmp6InDestUnreachs =     0     icmp6InAdminProhibs =     0
        .
        .
        icmp6OutGroupQueries=     0     icmp6OutGroupResps  =     2
        icmp6OutGroupReds   =     0

IGMP:
      12287 messages received
          0 messages received with too few bytes
          0 messages received with bad checksum
      12287 membership queries received
SCTP  sctpRtoAlgorithm     =  vanj
      sctpRtoMin           =  1000
      sctpRtoMax           = 60000
      sctpRtoInitial       =  3000
      sctpTimHearBeatProbe =     2
      sctpTimHearBeatDrop  =     0
      sctpListenDrop       =     0
      sctpInClosed         =     0
```

▼ So zeigen Sie den Status von Transportprotokollen an

Mit dem Befehl `netstat` können Sie den Status der Transportprotokolle anzeigen. Ausführliche Informationen finden Sie in der Manpage `netstat(1M)`.

1. **Zeigen Sie den Status der Transportprotokolle TCP und SCTP auf einem System an.**

   ```
   $ netstat
   ```

2. **Zeigen Sie den Status eines bestimmten Transportprotokolls auf einem System an.**

   `$ netstat -P` *transport-protocol*

   Werte für die Variable *Transportprotokoll* sind z. B. `tcp`, `sctp` oder `udp`.

Beispiel 8–6 Anzeigen des Status der Transportprotokolle TCP und SCTP

Das folgende Beispiel zeigt die Ausgabe des allgemeinen Befehls `netstat.` Beachten Sie, dass nur IPv4-Informationen angezeigt werden.

```
$ netstat

TCP: IPv4
   Local Address     Remote Address    Swind Send-Q  Rwind Recv-Q      State
----------------- -------------------- ----- ------  ----- ------     -------
lhost-1.login      abc.def.local.Sun.COM.980 49640      0     49640     0 ESTABLISHED
```

```
lhost-1.login      ghi.jkl.local.Sun.COM.1020 49640     1     49640    0 ESTABLISHED
remhost-1.1014     mno.pqr.remote.Sun.COM.nfsd 49640    0     49640    0 TIME_WAIT
SCTP:
Local Address    Remote Address  Swind  Send-Q  Rwind  Recv-Q StrsI/O  State
---------------- --------------  -----  ------ ------ ------  ------   -------
 *.echo            0.0.0.0           0       0 102400      0   128/1   LISTEN
 *.discard         0.0.0.0           0       0 102400      0   128/1   LISTEN
 *.9001            0.0.0.0           0       0 102400      0   128/1   LISTEN
```

Beispiel 8–7 Anzeigen des Status eines bestimmten Transportprotokolls

Das folgende Beispiel zeigt die Ausgabe, wenn Sie die Option `-P` mit dem Befehl `netstat` angeben.

```
$ netstat -P tcp

TCP: IPv4
   Local Address     Remote Address    Swind Send-Q  Rwind Recv-Q      State
---------------- ------------------- ----- ------  ----- ------     -------
lhost-1.login      abc.def.local.Sun.COM.980 49640      0     49640    0 ESTABLISHED
lhost.login        ghi.jkl.local.Sun.COM.1020 49640     1     49640    0 ESTABLISHED
remhost.1014       mno.pqr.remote.Sun.COM.nfsd 49640    0     49640    0 TIME_WAIT

TCP: IPv6
 Local Address    Remote Address        Swind Send-Q Rwind Recv-Q   State If
--------------- --------------------- ------ ----- ------ ----------- -----
localhost.38983   localhost.32777       49152      0 49152      0 ESTABLISHED
localhost.32777   localhost.38983       49152      0 49152      0 ESTABLISHED
localhost.38986   localhost.38980       49152      0 49152      0 ESTABLISHED
```

▼ So zeigen Sie den Netzwerkschnittstellenstatus an

Mit der Option `i` des Befehls `netstat` zeigen Sie den Status der Netzwerkschnittstellen an, die im lokalen System konfiguriert wurden. So können Sie die Anzahl der Pakete ermitteln, die ein System in jedem Netzwerk empfängt und sendet.

- **Zeigen Sie den Status der Netzwerkschnittstelle an.**

```
$ netstat -i
```

Beispiel 8–8 Anzeige des Netzwerkschnittstellenstatus

Das nächste Beispiel zeigt den Status des IPv4- und IPv6-Paketflusses durch die Schnittstellen des Hosts.

Beispielsweise kann der Zähler für eingehende Pakete (`Ipkts`) eines Servers jedes Mal um eins erhöht werden, wenn ein Client zu booten versucht, während der Zähler für abgehende Pakete (`Opkts`) konstant bleibt. Dieses Ergebnis deutet darauf hin, dass der Server die Boot-Anforderungspakete der Client empfängt. Jedoch weiß der Server nicht, wie er auf diese Pakete antworten soll. Dieses Fehlverhalten könnte durch eine falsche Adresse in einer der Datenbanken `hosts`, `ipnodes` oder `ethers` verursacht werden.

Bleibt der Zähler für eingehende Pakete jedoch konstant, sieht der Computer überhaupt keine Pakete. Dieses Ergebnis deutet auf einen anderen Fehler hin, möglicherweise ein Hardwareproblem.

```
Name  Mtu  Net/Dest      Address        Ipkts  Ierrs Opkts  Oerrs Collis Queue
lo0   8232 loopback      localhost      142    0     142    0     0      0
hme0  1500 host58        host58        1106302 0     52419  0     0      0

Name  Mtu  Net/Dest      Address                    Ipkts  Ierrs Opkts  Oerrs Collis
lo0   8252 localhost     localhost                   142    0     142    0     0
hme0  1500 fe80::a00:20ff:feb9:4c54/10 fe80::a00:20ff:feb9:4c54 1106305 0 52422 0  0
```

So zeigen Sie den Status der Sockets an

Mit der Option `-a` des Befehls `netstat` können Sie den Status der Sockets auf dem lokalen Host anzeigen.

- **Geben Sie den folgenden Befehl ein, um den Status der Sockets und die Routing-Tabelleneinträge anzuzeigen:**

  Zum Ausführen dieser Option von `netstat` können Sie Ihr Benutzerkonto verwenden.

  ```
  % netstat -a
  ```

Beispiel 8–9 Anzeigen aller Socket und Routing-Tabelleneinträge

Die Ausgabe des Befehls `netstat -a` zeigt umfangreiche Statistiken an. Das folgende Beispiel zeigt Teile einer typischen Ausgabe des Befehls `netstat -a`.

```
UDP: IPv4
   Local Address         Remote Address     State
-------------------- -------------------- -------
      *.bootpc                              Idle
host85.bootpc                               Idle
      *.*                                   Unbound
      *.*                                   Unbound
      *.sunrpc                              Idle
      *.*                                   Unbound
      *.32771                               Idle
      *.sunrpc                              Idle
      *.*                                   Unbound
      *.32775                               Idle
      *.time                                Idle
        .
        .
      *.daytime                             Idle
      *.echo                                Idle
      *.discard                             Idle

UDP: IPv6
   Local Address                     Remote Address                   State      If
--------------------------------- --------------------------------- ---------- -----
```

```
      *.*                                                     Unbound
      *.*                                                     Unbound
      *.sunrpc                                                Idle
      *.*                                                     Unbound
      *.32771                                                 Idle
      *.32778                                                 Idle
      *.syslog                                                Idle
      .
      .
TCP: IPv4
   Local Address        Remote Address    Swind Send-Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- ------ -------
      *.*                  *.*                0      0 49152      0 IDLE
localhost.4999             *.*                0      0 49152      0 LISTEN
      *.sunrpc             *.*                0      0 49152      0 LISTEN
      *.*                  *.*                0      0 49152      0 IDLE
      *.sunrpc             *.*                0      0 49152      0 LISTEN
      .
      .
      *.printer            *.*                0      0 49152      0 LISTEN
      *.time               *.*                0      0 49152      0 LISTEN
      *.daytime            *.*                0      0 49152      0 LISTEN
      *.echo               *.*                0      0 49152      0 LISTEN
      *.discard            *.*                0      0 49152      0 LISTEN
      *.chargen            *.*                0      0 49152      0 LISTEN
      *.shell              *.*                0      0 49152      0 LISTEN
      *.shell              *.*                0      0 49152      0 LISTEN
      *.kshell             *.*                0      0 49152      0 LISTEN
      *.login
       .
       .
            *.*                 0      0 49152      0 LISTEN
   *TCP: IPv6
 Local Address             Remote Address       Swind Send-Q Rwind Recv-Q   State If
----------------------- ----------------------- ----- ------ ----- ------    ----
   *.*                         *.*                0      0 49152      0      IDLE
   *.sunrpc                    *.*                0      0 49152      0      LISTEN
   *.*                         *.*                0      0 49152      0      IDLE
   *.32774                     *.*                0      0 49152
```

So zeigen Sie den Status von Paketübertragungen eines bestimmten Adresstyps an

Mit der Option `-f` des Befehls `netstat` können Sie Statistiken zu den Paketübertragungen einer bestimmten Adressfamilie anzeigen.

- **Zeigen Sie die Statistiken entweder von IPv4- oder von IPv6-Paketübertragungen an.**

  `$ netstat -f` *inet* | *inet6*

  Zum Anzeigen von Informationen zu IPv4-Übertragungen geben Sie `inet` als Argument für `netstat -f` ein. Zum Anzeigen von Informationen zu IPv6-Übertragungen geben Sie `inet6` als Argument für `netstat -f` ein.

Beispiel 8–10 Status von IPv4-Paketübertragungen

Das folgende Beispiel zeigt die Ausgabe des Befehls `netstat -f inet`.

```
TCP: IPv4
   Local Address        Remote Address    Swind Send-Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- ------ -------
host58.734          host19.nfsd       49640      0 49640      0 ESTABLISHED
host58.38063        host19.32782      49640      0 49640      0 CLOSE_WAIT
host58.38146        host41.43601      49640      0 49640      0 ESTABLISHED
host58.996          remote-host.login 49640      0 49206      0 ESTABLISHED
```

Beispiel 8–11 Status von IPv6-Paketübertragungen

Das folgende Beispiel zeigt die Ausgabe des Befehls `netstat -f inet6`.

```
TCP: IPv6
 Local Address          Remote Address        Swind Send-Q Rwind Recv-Q   State    If
------------------ ------------------------- ----- ------ ----- ------ --------- -----
localhost.38065         localhost.32792       49152   0 49152      0    ESTABLISHED
localhost.32792         localhost.38065       49152   0 49152      0    ESTABLISHED
localhost.38089         localhost.38057       49152   0 49152      0    ESTABLISHED
```

▼ So zeigen Sie den Status bekannter Routen an

Mit der Option `-r` des Befehls `netstat` zeigen Sie die Routing-Tabelle des lokalen Hosts an. Diese Tabelle zeigt den Status aller dem Host bekannten Routen. Sie können diese Option des Befehls `netstat` von Ihrem Benutzerkonto aus ausführen.

- **Zeigen Sie die IP-Routing Tabelle an.**

```
$ netstat -r
```

Beispiel 8–12 Ausgabe der Routing-Tabelle des Befehls `netstat`

Das folgende Beispiel zeigt die Ausgabe des Befehls `netstat -r`.

```
Routing Table: IPv4
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
host15               myhost               U         1  31059  hme0
10.0.0.14            myhost               U         1      0  hme0
default              distantrouter        UG        1      2  hme0
localhost            localhost            UH        42019361  lo0

Routing Table: IPv6
  Destination/Mask            Gateway                   Flags Ref   Use   If
--------------------------- --------------------------- ----- --- ------ -----
2002:0a00:3010:2::/64    2002:0a00:3010:2:1b2b:3c4c:5e6e:abcd U  1      0 hme0:1
fe80::/10                fe80::1a2b:3c4d:5e6f:12a2    U       1     23 hme0
ff00::/8                 fe80::1a2b:3c4d:5e6f:12a2    U       1      0 hme0
```

```
default                  fe80::1a2b:3c4d:5e6f:12a2    UG      1      0 hme0
localhost                localhost                   UH      9  21832 lo0
```

In der folgenden Tabelle wird die Bedeutung der verschiedenen Parameter der Bildschirmausgabe des Befehls `netstat –r` beschrieben.

Parameter	Beschreibung
`Destination` `Destination/Mask`	Gibt den Host an, der als Ziel-Endpunkt der Route fungiert. Beachten Sie, dass die IPv6-Routing-Tabelle das Präfix für einen 6to4-Tunnelendpunkt (`2002:0a00:3010:2::/64`) als Ziel-Endpunkt der Route anzeigt.
`Gateway`	Gibt das zum Weiterleiten von Paketen zu verwendende Gateway an.
`Flags`	Zeigt den aktuellen Status der Route an. Das Flag `U` gibt an, dass die Route hochgefahren ist. Das Flag `G` gibt an, dass die Route zu einem Gateway führt.
`Use`	Zeigt die Anzahl der gesendeten Pakete an.
`Interface`	Zeigt die Schnittstelle auf dem lokalen Host an, die als Ursprungs-Endpunkt der Übertragung dient.

Ermitteln des Status von Remote-Hosts mit dem Befehl `ping`

Mit dem Befehl `ping` können Sie den Status eines Remote-Hosts ermitteln. Wenn Sie den Befehl `ping` ausführen, sendet das ICMP-Protokoll ein Datagramm an den angegebenen Host und fordert eine Antwort an. ICMP ist das Protokoll, das in einem TCP/IP-Netzwerk für die Fehlerbehandlung verantwortlich ist. Mit dem Befehl `ping` können Sie feststellen, ob eine IP-Verbindung zum angegebenen Remote-Host besteht.

Im Folgenden ist die allgemeine Syntax des Befehls `ping` aufgeführt:

`/usr/sbin/ping` *Host [Timeout]*

In dieser Syntax ist *Host* der Name des Remote-Hosts. Das optionale Argument *Timeout* gibt eine Zeit in Sekunden an, über die der Befehl `ping` versucht, den Remote-Host zu erreichen. Der Standardwert beträgt 20 Sekunden. Weitere Informationen zur Syntax und den gültigen Optionen finden Sie in der Manpage `ping`(1M).

▼ So ermitteln Sie, ob ein Remote-Host ausgeführt wird

- **Geben Sie den Befehl `ping` in der folgenden Form ein:**

  `$` **`ping`** *hostname*

Wenn der Host *Hostname* ICMP-Übertragungen akzeptiert, wird die folgende Meldung angezeigt:

```
hostname is alive
```

Diese Meldung zeigt, dass *Hostname* auf die ICMP-Anforderung reagiert. Wenn *Hostname* jedoch heruntergefahren ist oder keine ICMP-Pakete empfangen kann, erhalten Sie die folgende Antwort vom ping-Befehl:

```
no answer from hostname
```

So stellen Sie fest, ob ein Host Pakete abwirft

Mit der Option -s des Befehls ping können Sie feststellen, ob ein Remote-Host zwar ausgeführt wird, aber dennoch Pakete verliert.

- **Geben Sie den Befehl ping in der folgenden Form ein:**

```
$ ping -s hostname
```

Beispiel 8–13 ping-Ausgabe zur Erkennung abgeworfener Pakete

Der Befehl ping -s *Hostname* sendet kontinuierlich Pakete an den angegebenen Host, bis ein Interrupt-Zeichen gesendet wird oder ein Timeout eintritt. Die Antworten auf Ihren Bildschirm sollten etwa wie folgt aussehen:

```
& ping -s host1.domain8
PING host1.domain8 : 56 data bytes
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=0. time=1.67 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=1. time=1.02 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=2. time=0.986 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=3. time=0.921 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=4. time=1.16 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=5. time=1.00 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=5. time=1.980 ms

^C

----host1.domain8  PING Statistics----
7 packets transmitted, 7 packets received, 0% packet loss
round-trip (ms)  min/avg/max/stddev = 0.921/1.11/1.67/0.26
```

Die Paketverluststatistiken geben an, ob der Host Pakete verloren hat. Falls der Befehl ping fehlschlägt, prüfen Sie den Netzwerkstatus, der von den Befehlen ifconfig und netstat gemeldet wird. Lesen Sie dazu auch „Überwachen der Schnittstellenkonfiguration mit dem Befehl ifconfig“ auf Seite 221 und „Überwachen des Netzwerkstatus mit dem Befehl netstat“ auf Seite 225.

Verwalten und Protokollieren der Netzwerkstatusanzeigen

Die folgenden Aufgaben zeigen, wie Sie den Netzwerkstatus mit bekannten Netzwerkbefehlen prüfen.

▼ So steuern Sie die Anzeige der Ausgabe von IP-bezogenen Befehlen

Sie können die Ausgabe der Befehle `netstat` und `ifconfig` so steuern, dass nur IPv4- oder sowohl IPv4- und IPv6-Informationen angezeigt werden.

1. **Erstellen Sie die `/etc/default/inet_type`-Datei.**

2. **Fügen Sie einen der folgenden Einträge zur `/etc/default/inet_type`-Datei hinzu, je nachdem, welche Angabe für Ihr Netzwerk erforderlich ist:**

   - So zeigen Sie nur IPv4-Informationen an:

     ```
     DEFAULT_IP=IP_VERSION4
     ```

   - So zeigen Sie sowohl IPv4- als auch IPv6-Informationen an

     ```
     DEFAULT_IP=BOTH
     ```

     oder

     ```
     DEFAULT_IP=IP_VERSION6
     ```

   Weitere Informationen zur `inet_type`-Datei finden Sie in der Manpage `inet_type(4)`.

Hinweis – Die Flags `-4` und `-6` im Befehl `ifconfig` setzen die Werte in der `inet_type`-Datei außer Kraft. Darüber hinaus überschreibt das Flag `-f` im Befehl `netstat` die Werte in der `inet_type`-Datei.

Beispiel 8–14 Steuern der Ausgabe zur Auswahl von IPv4- und IPv6-Informationen

- Wenn Sie die Variable `DEFAULT_IP=BOTH` oder `DEFAULT_IP=IP_VERSION6` in der `inet_type`-Datei angeben, sollte die folgende Ausgabe angezeigt werden:

  ```
  % ifconfig -a
  lo0: flags=1000849 mtu 8232 index 1
          inet 10.10.0.1 netmask ff000000
  qfe0: flags=1000843 mtu 1500 index 2
          inet 10.46.86.54 netmask ffffff00 broadcast 10.46.86.255
          ether 8:0:20:56:a8
  lo0: flags=2000849 mtu 8252 index 1
          inet6 ::1/128
  qfe0: flags=2000841 mtu 1500 index 2
  ```

```
        ether 8:0:20:56:a8
        inet6 fe80::a00:fe73:56a8/10
qfe0:1: flags=2080841 mtu 1500 index 2
        inet6 2001:db8:3c4d:5:a00:fe73:56a8/64
```

- Wenn Sie die Variable `DEFAULT_IP=IP_VERSION4` oder `DEFAULT_IP=IP_VERSION6` in der `inet_type`-Datei angeben, sollten die folgende Ausgabe angezeigt werden:

```
% ifconfig -a
lo0: flags=849 mtu 8232
        inet 10.10.0.1 netmask ff000000
qfe0: flags=843 mtu 1500
        inet 10.46.86.54 netmask ffffff00 broadcast 10.46.86.255
        ether 8:0:20:56:a8
```

So protokollieren Sie die Aktionen des IPv4-Routing-Daemon

Wenn Sie eine Fehlfunktion des IPv4-Routing-Daemons `routed` vermuten, können Sie ein Protokoll starten, das die Aktivitäten des Daemon aufzeichnet. Das Protokoll enthält alle Paketübertragungen, die nach dem Start des `routed`-Daemon ausgeführt wurden.

1. **Nehmen Sie auf dem lokalen Host die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Erstellen Sie eine Protokolldatei, in der die Aktionen des Routing-Daemons aufgezeichnet werden:**

   `# /usr/sbin/in.routed /var/`*log-file-name*

Achtung – Bei einem stark ausgelasteten Netzwerk kann dieser Befehl eine extrem umfangreiche Ausgabe erzeugen.

Beispiel 8–15 Netzwerkprotokoll für den `in.routed`-Daemon

Das folgende Beispiel zeigt den Anfang des Protokolls, das nach dem Verfahren unter „So protokollieren Sie die Aktionen des IPv4-Routing-Daemon“ auf Seite 235 erstellt wurde.

```
-- 2003/11/18 16:47:00.000000 --
Tracing actions started
RCVBUF=61440
Add interface lo0  #1   127.0.0.1      -->127.0.0.1/32
   <UP|LOOPBACK|RUNNING|MULTICAST|IPv4> <PASSIVE>
```

```
Add interface hme0 #2   10.10.48.112    -->10.10.48.0/25
    <UP|BROADCAST|RUNNING|MULTICAST|IPv4>
turn on RIP
Add    10.0.0.0        -->10.10.48.112      metric=0  hme0  <NET_SYN>
Add    10.10.48.85/25  -->10.10.48.112      metric=0  hme0  <IF|NOPROP>
```

▼ So verfolgen Sie die Aktivitäten des IPv6 Neighbor Discovery-Daemon

Wenn Sie eine Fehlfunktion des `in.ndpd`-Daemons vermuten, können Sie ein Protokoll starten, das die Aktivitäten des Daemon aufzeichnet. Diese Ablaufverfolgung wird bis zur Beendigung in der standardmäßigen Ausgabe angezeigt. Dieses Protokoll enthält alle Paketübertragungen, die nach dem Start des `in.ndpd`-Daemon ausgeführt wurden.

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser bei dem lokalen IPv6-Knoten an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Starten Sie eine Verfolgung des `in.ndpd`-Daemon.**

   ```
   # /usr/lib/inet/in.ndpd -t
   ```

3. **Beenden Sie die Verfolgung gegebenenfalls durch Drücken von Strg-C.**

Beispiel 8–16 Verfolgung des `in.ndpd`-Daemon

Die folgende Ausgabe zeigt den Beginn der Verfolgung des `in.ndpd`-Daemon.

```
# /usr/lib/inet/in.ndpd -t
Nov 18 17:27:28 Sending solicitation to  ff02::2 (16 bytes) on hme0
Nov 18 17:27:28         Source LLA: len 6 <08:00:20:b9:4c:54>
Nov 18 17:27:28 Received valid advert from fe80::a00:20ff:fee9:2d27 (88 bytes) on hme0
Nov 18 17:27:28         Max hop limit: 0
Nov 18 17:27:28         Managed address configuration: Not set
Nov 18 17:27:28         Other configuration flag: Not set
Nov 18 17:27:28         Router lifetime: 1800
Nov 18 17:27:28         Reachable timer: 0
Nov 18 17:27:28         Reachable retrans timer: 0
Nov 18 17:27:28         Source LLA: len 6 <08:00:20:e9:2d:27>
Nov 18 17:27:28         Prefix: 2001:08db:3c4d:1::/64
Nov 18 17:27:28                 On link flag:Set
Nov 18 17:27:28                 Auto addrconf flag:Set
Nov 18 17:27:28                 Valid time: 2592000
Nov 18 17:27:28                 Preferred time: 604800
Nov 18 17:27:28         Prefix: 2002:0a00:3010:2::/64
Nov 18 17:27:28                 On link flag:Set
```

```
Nov 18 17:27:28                Auto addrconf flag:Set
Nov 18 17:27:28                Valid time: 2592000
Nov 18 17:27:28                Preferred time: 604800
```

Anzeigen von Routing-Informationen mit dem Befehl traceroute

Mit dem Befehl `traceroute` zeichnen Sie die Route auf, der ein IP-Paket zu einem Remote-System folgt. Technische Informationen zum Befehl `traceroute` finden Sie in der Manpage `traceroute`(1M).

Mit dem Befehl `traceroute` können Sie alle falschen Routing-Konfigurationen und mögliche Probleme im Routing-Pfad aufdecken. Ist ein bestimmter Host nicht erreichbar, können Sie mit `traceroute` feststellen, welchen Pfad das Paket zum Remote-Host eingeschlagen hat, und wo mögliche Probleme aufgetreten sind.

Der Befehl `traceroute` kann auch zur Anzeige der Round-Trip-Zeit jedes Gateway im Pfad zum Ziel-Host verwendet werden. Mit diesen Informationen kann beispielsweise analysiert werden, warum der Datenverkehr zwischen den beiden Hosts nur langsam erfolgt.

▼ So ermitteln Sie die Route zu einem Remote-Host

- **Geben Sie den folgenden Befehl ein, um die Route zu einem Remote-System zu ermitteln:**

  `%` **`traceroute`** *destination-hostname*

  Sie können den Befehl `traceroute` in diesem Format von Ihrem Benutzerkonto aus ausführen.

Beispiel 8–17 Verwenden des Befehls `traceroute` zum Anzeigen der Route zu einem Remote-Host

Die folgende Ausgabe des Befehls `traceroute` zeigt einen Pfad mit sieben Hops an, den ein Paket vom lokalen System `nearhost` zum Remote-System `farhost` eingeschlagen hat. Darüber hinaus zeigt die Ausgabe, wie lange ein Paket bis zur jeweils nächsten Hop benötigt.

```
istanbul% traceroute farhost.faraway.com
    traceroute to farhost.faraway.com (172.16.64.39), 30 hops max, 40 byte packets
     1  frbldg7c-86 (172.16.86.1)  1.516 ms  1.283 ms  1.362 ms
     2  bldg1a-001 (172.16.1.211)  2.277 ms  1.773 ms  2.186 ms
     3  bldg4-bldg1 (172.16.4.42)  1.978 ms  1.986 ms  13.996 ms
     4  bldg6-bldg4 (172.16.4.49)  2.655 ms  3.042 ms  2.344 ms
     5  ferbldg11a-001 (172.16.1.236)  2.636 ms  3.432 ms  3.830 ms
     6  frbldg12b-153 (172.16.153.72)  3.452 ms  3.146 ms  2.962 ms
     7  sanfrancisco (172.16.64.39)  3.430 ms  3.312 ms  3.451 ms
```

So verfolgen Sie alle Routen

Bei diesem Verfahren wird die Option -a des Befehls traceroute verwendet, um alle Routen zu verfolgen.

- **Geben Sie den folgenden Befehl auf dem lokalen System ein:**

  % **traceroute -a***host-name*

  Sie können den Befehl traceroute in diesem Format von Ihrem Benutzerkonto aus ausführen.

Beispiel 8–18 Verfolgen aller Routen zu einem Dual-Stack-Host

In diesem Beispiel werden alle möglichen Routen zu einem Dual-Stack-Host gezeigt.

```
% traceroute -a v6host.remote.com
traceroute: Warning: Multiple interfaces found; using 2::56:a0:a8 @ eri0:2
traceroute to v6host (2001:db8:4a3b::102:a00:fe79:19b0),30 hops max, 60 byte packets
 1  v6-rout86 (2001:db8:4a3b:56:a00:fe1f:59a1)  35.534 ms  56.998 ms *
 2  2001:db8::255:0:c0a8:717  32.659 ms  39.444 ms *
 3  farhost.faraway.COM (2001:db8:4a3b::103:a00:fe9a:ce7b)  401.518 ms  7.143 ms *
 4  distant.remote.com (2001:db8:4a3b::100:a00:fe7c:cf35)  113.034 ms  7.949 ms *
 5  v6host (2001:db8:4a3b::102:a00:fe79:19b0)  66.111 ms *  36.965 ms

traceroute to v6host.remote.com  (192.168.10.75),30 hops max,40 byte packets
 1  v6-rout86 (172.16.86.1)  4.360 ms  3.452 ms  3.479 ms
 2  flrmpj17u.here.COM (172.16.17.131)  4.062 ms  3.848 ms  3.505 ms
 3  farhost.farway.com (10.0.0.23)  4.773 ms *  4.294 ms
 4  distant.remote.com (192.168.10.104)  5.128 ms  5.362 ms *
 5  v6host  (192.168.15.85)  7.298 ms  5.444 ms *
```

Überwachen der Paketübertragungen mit dem Befehl snoop

Mit dem Befehl snoop können Sie den Status der Datenübertragungen überwachen. snoop erfasst Netzwerkpakete und zeigt deren Inhalte in dem von Ihnen geforderten Format an. Pakete können entweder direkt nach dem Empfang angezeigt oder in einer Datei gespeichert werden. Wenn der Befehl snoop in eine Datei schreibt, sind Paketverluste aufgrund hoher Auslastung während der Verfolgung unwahrscheinlich. snoop wird dann zum Auswerten des Dateiinhalts verwendet.

Zum Erfassen von Paketen, die im promiskuitiven Modus von der Standardschnittstelle empfangen oder gesendet werden, müssen Sie die Rolle eines Netzwerkmanagers annehmen oder sich als Superuser anmelden. snoop kann nur die Daten in einer Zusammenfassung anzeigen, die auf der höchsten Protokollebene bleiben. Beispielsweise kann ein NFS-Paket nur NFS-Informationen anzeigen. Die zu Grunde liegenden RPC-, UDP-, IP- und Ethernet Frame-Informationen werden unterdrückt, können aber angezeigt werden, wenn eine der verbose-Optionen gewählt wird.

Arbeiten Sie regelmäßig mit dem Befehl snoop, um sich mit seinem normalen Systemverhalten vertraut zu machen. Hilfe zur Analyse von Paketen finden Sie in den aktuellen Weißbüchern und RFCs, suchen Sie den Rat eines Experten in den jeweiligen Bereichen, z. B. NFS oder NIS. Weitere Informationen zur Syntax von snoop und den gültigen Optionen finden Sie in der Manpage snoop(1M)

▼ So prüfen Sie Pakete von allen Schnittstellen

1. **Nehmen Sie auf dem lokalen Host die Rolle eines Netzwerkmanagers an, oder melden Sie sich als Superuser an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Drucken Sie Informationen zu den Schnittstellen, die an das System angehängt sind.**

   ```
   # ifconfig -a
   ```

   In der Regel verwendet der Befehl snoop das erste nicht-Loopback-Gerät, normalerweise die primäre Netzwerkschnittstelle.

3. **Beginnen Sie die Paketerfassung durch Eingabe von snoop ohne zusätzliche Argumente. Siehe Beispiel 8–19.**

4. **Drücken Sie Strg-C, um den Prozess zu unterbrechen.**

Beispiel 8–19 Ausgabe des Befehls snoop

Der allgemeine snoop-Befehl bei einem Dual-Stack-Host eine Ausgabe wieder, die etwa der Folgenden entspricht.

```
% snoop
Using device /dev/hme (promiscuous mode)
farhost.remote.com -> myhost       RLOGIN C port=993
    myhost -> farhost.remote.com   RLOGIN R port=993 Using device /dev/hme
router5.local.com -> router5.local.com ARP R 10.0.0.13, router5.local.com is
    0:10:7b:31:37:80
router5.local.com -> BROADCAST     TFTP Read "network-confg" (octet)
farhost.remote.com -> myhost       RLOGIN C port=993
    myhost ->   nisserve2          NIS C MATCH 10.0.0.64 in ipnodes.byaddr
nisserve2 ->    myhost             NIS R MATCH No such key
    blue-112 -> slave-253-2        NIS C MATCH 10.0.0.112 in ipnodes.byaddr
myhost -> DNSserver.local.com      DNS C 192.168.10.10.in-addr.arpa. Internet PTR ?
DNSserver.local.com  myhost        DNS R 192.168.10.10.in-addr.arpa. Internet PTR
   niserve2.
.
.
farhost.remote.com-> myhost        RLOGIN C port=993
```

```
    myhost -> farhost.remote.com   RLOGIN R port=993 fe80::a00:20ff:febb:
.
fe80::a00:20ff:febb:e09 -> ff02::9 RIPng R (5 destinations)
```

Die in dieser Ausgabe erfassten Pakete zeigen einen Bereich mit einer Remote-Anmeldung, einschließlich Lookup-Vorgängen an die NIS- und DNS-Servern zur Auflösung der Adresse. Darüber hinaus sind regelmäßig auftretende ARP-Pakete von lokalen Router und Advertisement-Nachrichten der Link-lokalen IPv6-Adresse an `in.ripngd` enthalten.

▼ So erfassen Sie die Ausgabe des Befehls `snoop` in einer Datei

1 Nehmen Sie auf dem lokalen Host die Rolle eines Netzwerkmanagers an, oder melden Sie sich als Superuser an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2 Erfassen Sie eine `snoop`-Sitzung in einer Datei.

\# **snoop -o** *filename*

Beispiel:

```
# snoop -o /tmp/cap
Using device /dev/eri (promiscuous mode)
30 snoop: 30 packets captured
```

In diesem Beispiel wurden 30 Pakete in einer Datei namens `/tmp/cap` erfasst. Dieser Datei kann sich in jedem Verzeichnis mit ausreichend Speicherplatz befinden. Die Anzahl der erfassten Pakete wird in der Befehlszeile angezeigt. Anschließend können Sie jederzeit Strg-C drücken, um die Erfassung abzubrechen.

`snoop` erzeugt eine spürbare Netzwerklast auf dem Host-Computer, die zu einer Verzerrung der Ergebnisse führen kann. Um die tatsächlichen Ergebnisse anzuzeigen, führen Sie `snoop` von einem dritten System aus.

3 Zeigen Sie die Ausgabe des Befehls `snoop` in der Datei an.

\# **snoop -i** *filename*

Beispiel 8–20 Inhalt einer Datei zur Erfassung der Ausgabe des Befehls `snoop`

Die folgende Ausgabe zeigt verschiedene Informationen an, die Sie als Ausgabe des Befehls `snoop -i` erhalten könnten.

```
# snoop -i /tmp/cap
1   0.00000 fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fecd:4375
    ICMPv6 Neighbor advertisement
2   0.16198 farhost.com   -> myhost     RLOGIN C port=985
3   0.00008 myhost -> farhost.com       RLOGIN R port=985
10  0.91493    10.0.0.40 -> (broadcast)  ARP C Who is 10.0.0.40, 10.0.0.40 ?
34  0.43690 nearserver.here.com  -> 224.0.1.1  IP  D=224.0.1.1 S=10.0.0.40 LEN=28,
      ID=47453, TO =0x0, TTL=1
35  0.00034  10.0.0.40 -> 224.0.1.1    IP  D=224.0.1.1 S=10.0.0.40 LEN=28, ID=57376,
     TOS=0x0, TTL=47
```

▼ So prüfen Sie Pakete zwischen einem IPv4-Server und einem Client

1. **Richten Sie ein von einem Hub getrenntes `snoop`-System ein, das entweder mit dem Client oder dem Server verbunden ist.**

   Das dritte System (das `snoop`-System) prüft den gesamten zwischengeschalteten Verkehr, so dass die `snoop`-Verfolgung widerspiegelt, was tatsächlich in der Leitung geschieht.

2. **Nehmen Sie auf dem `snoop`-System die Rolle eines Netzwerkmanagers an, oder melden Sie sich als Superuser an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

3. **Geben Sie den `snoop`-Befehl mit den gewünschten Optionen ein, und speichern Sie die Ausgabe in einer Datei.**

4. **Prüfen und analysieren Sie die Ausgabe.**

   Informationen zur `snoop`-Erfassungsdatei finden Sie unter RFC 1761, Snoop Version 2 Packet Capture File Format (`http://www.ietf.org/rfc/rfc1761.txt?number=1761snoop`).

▼ So überwachen Sie den IPv6-Netzwerkverkehr

Mit dem `snoop`-Befehl können Sie auch nur IPv6-Pakete anzeigen.

1. **Nehmen Sie auf dem lokalen Knoten die Rolle eines Netzwerkmanagers an, oder melden Sie sich als Superuser an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Erfassen Sie IPv6-Pakete.

```
# snoop ip6
```

Weitere Informationen zum Befehl `snoop` finden Sie in der Manpage `snoop`(1M).

Beispiel 8–21 Anzeigen von ausschließlich IPv6-Netzwerkverkehr

Das folgende Beispiel zeigt eine typische Ausgabe, wenn der Befehl `snoop ip6` auf einem Knoten ausgeführt wird.

```
# snoop ip6
fe80::a00:20ff:fecd:4374 -> ff02::1:ffe9:2d27 ICMPv6 Neighbor solicitation
fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fecd:4375 ICMPv6 Neighbor
      solicitation
fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fecd:4375 ICMPv6 Neighbor
      solicitation
fe80::a00:20ff:febb:e09 -> ff02::9      RIPng R (11 destinations)
fe80::a00:20ff:fee9:2d27 -> ff02::1:ffcd:4375 ICMPv6 Neighbor solicitation
```

Verwaltuen der standardmäßigen Adressauswahl

Oracle Solaris erlaubt, dass eine Schnittstelle über mehrere IP-Adressen verfügt. Technologien wie z. B. Network Multipathing (IPMP) ermöglichen es, dass mehrere Netzwerkschnittstellenkarten (NICs) mit der gleichen IP-Sicherungsschicht verbunden werden. Diese Verbindung kann über mehrere IP-Adressen verfügen. Darüber hinaus verfügen Schnittstellen auf IPv6-konformen Systemen über eine Link-lokale IPv6-Adresse, mindestens eine IPv6-Routing-Adresse und eine IPv4-Adresse für mindestens eine Schnittstelle.

Wenn das System eine Transaktionen eingeleitet, ruft eine Anwendung den Socket `getaddrinfo` auf. `getaddrinfo` erfasst die Adresse, die möglicherweise auf dem Zielsystem verwendet wird. Anschließend ordnet der Kernel diese Liste nach Vorrangigkeit, um das beste Ziel für das Paket herauszufinden. Dieser Prozess wird als *Zieladressensortierung* bezeichnet. Dann wählt der Oracle Solaris-Kernel anhand der besten Zieladresse für das Paket das geeignete Format für die Quelladresse aus. Dieser Prozess wird als *Adressauswahl* bezeichnet. Weitere Informationen zur Zieladresssortierung finden Sie in der Manpage `getaddrinfo`(3SOCKET).

Sowohl nur-IPv4- als auch Dual-Stack-IPv4/IPv6-Systeme müssen eine Standard-Adressauswahl ausführen. In den meisten Fällen müssen die standardmäßigen Mechanismen zur Adressauswahl nicht geändert werden. Eventuell müssen Sie jedoch die Priorität der Adressformate so ändern, so dass IPMP- oder 6to4-Adressformate bevorzugt werden.

So verwalten Sie die Richtlinientabelle zur IPv6-Adressauswahl

Im folgenden Verfahren wird beschrieben, wie Sie Änderungen an der Richtlinientabelle zur Adressauswahl vornehmen. Konzeptuelle Informationen zur Standard-IPv6-Adressauswahl finden Sie unter „ipaddrsel-Befehl“ auf Seite 289.

Achtung – Nehmen Sie keine Änderungen an der Richtlinientabelle zur IPv6-Adressauswahl vor, es sei denn, die im Folgenden aufgeführten Gründe lassen sich auf Ihr System anwenden. Andernfalls könnten Sie durch eine falsch aufgebaute Richtlinientabelle Probleme im Netzwerk verursachen. Denken Sie daran, eine Sicherheitskopie der Richtlinientabelle anzulegen. Dies wird im folgenden Verfahren beschrieben.

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Arbeiten Sie die Tabelle mit den aktuellen Richtlinien zur IPv6-Adressauswahl durch.**

```
# ipaddrsel
# Prefix                  Precedence Label
::1/128                           50 Loopback
::/0                              40 Default
2002::/16                         30 6to4
::/96                             20 IPv4_Compatible
::ffff:0.0.0.0/96                 10 IPv4
```

3. **Erstellen Sie eine Sicherungskopie der Richtliniendatei der Standardadressen.**

```
# cp /etc/inet/ipaddrsel.conf /etc/inet/ipaddrsel.conf.orig
```

4. **Fügen Sie Ihre Anpassungen mit einem Texteditor in die Datei `/etc/inet/ipaddrsel.conf` ein.**

   Verwenden Sie für Einträge in die Datei `/etc/inet/ipaddrsel` die folgende Syntax:

   prefix/prefix-length precedence label [# comment]

   Im Folgenden sind einige Änderungen aufgeführt, die an der Richtlinientabelle vorgenommen werden können:

   - Weisen Sie den 6to4-Adressen die höchste Priorität zu.

```
2002::/16                         50 6to4
::1/128                           45 Loopback
```

     Das 6to4-Adressenformat besitzt jetzt die höchste Priorität (50). Loopback, das vorher eine Prioriät von 50 hatte, besitzt jetzt die Priorität 45. Die anderen Adressformate bleiben gleich.

- Weisen Sie eine bestimmte Quelladresse zu, die bei der Kommunikation mit einer bestimmten Zieladresse verwendet wird.

  ```
  ::1/128                           50 Loopback
  2001:1111:1111::1/128             40 ClientNet
  2001:2222:2222::/48               40 ClientNet
  ::/0                              40 Default
  ```

  Dieser besondere Eintrag eignet sich für Hosts mit nur einer physikalischen Schnittstelle. Hier wird `2001:1111:1111::1/128` als Quelladresse für alle Pakete priorisiert, die an Ziele im Netzwerk `2001:2222:2222::/48` gesendet wurden. Die Priorität 40 erzeugt eine höhere Prioritätsstufe für die Quelladresse `2001:1111:1111::1/128` als andere Adressformate, die für die Schnittstelle konfiguriert wurden.

- Favorisieren Sie IPv4-Adressen gegenüber IPv6-Adressen.

  ```
  ::ffff:0.0.0.0/96                 60 IPv4
  ::1/128                           50 Loopback
  .
  .
  ```

  Die Prioritätsstufe des IPv4-Formats `::ffff:0.0.0.0/96` wurde von 10 zu 60 geändert, die höchste Priorität in der Tabelle.

5 Laden Sie die modifizierte Richtlinientabelle in den Kernel.

```
ipaddrsel -f /etc/inet/ipaddrsel.conf
```

6 Wenn die modifizierte Richtlinientabelle Probleme verursacht, stellen Sie die Richtlinientabelle für die standardmäßige IPv6-Adressauswahl wieder her.

```
# ipaddrsel -d
```

▼ So modifizieren Sie die IPv6-Adressauswahltabelle nur für die aktuelle Sitzung

Wenn Sie die `/etc/inet/ipaddrsel.conf`-Datei bearbeiten, werden alle vorgenommenen Änderungen auch nach einem Neustart beibehalten. Soll die modifizierte Richtlinientabelle nur während der aktuellen Sitzung gültig sein, führen Sie das folgende Verfahren aus.

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Kopieren Sie den Inhalt der Datei `/etc/inet/ipaddrsel` nach *Dateiname*, dabei stellt *Dateiname* einen Namen Ihrer Wahl dar.

```
# cp /etc/inet/ipaddrsel filename
```

3 **Ändern Sie die Richtlinientabelle in** *Dateiname* **Ihren Anforderungen entsprechend.**

4 **Laden Sie die modifizierte Richtlinientabelle in den Kernel.**

```
# ipaddrsel -f filename
```

Der Kernel verwendet die neue Richtlinientabelle, bis Sie das System neu booten.

KAPITEL 9

Fehlersuche bei Netzwerkproblemen (Aufgaben)

Dieses Kapitel enthält Lösungen für allgemeine Probleme, die in Ihrem Netzwerk auftreten könnten. Es umfasst die folgenden Themen:

- „Allgemeine Tipps zur Fehlersuche bei Netzwerkproblemen“ auf Seite 247
- „Allgemeine Probleme bei der Bereitstellung von IPv6“ auf Seite 249

Neuerungen in diesem Kapitel

Unter Solaris 10 7/07 wird die Datei `/etc/inet/ipnodes` nicht mehr benötigt. Verwenden Sie `/etc/inet/ipnodes` nur für frühere Oracle Solaris 10-Versionen, wie es in den jeweiligen Verfahren beschrieben wird.

Allgemeine Tipps zur Fehlersuche bei Netzwerkproblemen

Das erste Anzeichen eines Problems in einem Netzwerk ist, wenn mit einem oder mehreren Hosts kein Datenaustausch durchgeführt werden kann. Wenn ein Host nach dem Hinzufügen zu einem Netzwerk nicht online geschaltet werden kann, könnte der Fehler in einer der Konfigurationsdateien liegen. Möglich wäre aber auch eine fehlerhafte Netzwerkschnittstellenkarte. Wenn ein einzelner Host unvermittelt ein Problem erzeugt, könnte die Netzwerkschnittstelle die Ursache sein. Können die Hosts in einem Netzwerk zwar untereinander, aber nicht mit anderen Netzwerken kommunizieren, ist vermutlich der Router die Fehlerursache. Möglich wäre auch, dass das Problem in dem anderen Netzwerk liegt.

Mit dem Befehl `ifconfig` können Sie Informationen zu den Netzwerkschnittstellen abrufen. Der Befehl `netstat` eignet sich zum Anzeigen von Routing-Tabellen und Protokollstatistiken. Auch Netzwerk-Diagnoseprogramme von Drittanbietern enthalten Tools zur Fehlersuche. Weitere Informationen finden Sie in der Dokumentation der Drittanbieter.

Weniger offensichtlich sind die Ursachen von Problemen, die zu einer Leistungsverschlechterung im Netzwerk führen. Mit Tools wie `ping` können Sie Probleme wie den Verlust von Paketen durch einen Host feststellen.

Durchführen allgemeiner Diagnoseprüfungen

Bei Problemen im Netzwerk können Sie verschiedene Softwareprüfungen durchführen, um allgemeine Software-bezogene Probleme zu diagnostizieren und zu korrigieren.

▼ So führen Sie eine allgemeine Prüfung der Netzwerksoftware durch

1. **Nehmen Sie auf dem lokalen System die Rolle eines Netzwerkmanagers an, oder melden Sie sich als Superuser an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Zeigen Sie die Netzwerkinformationen mit dem Befehl `netstat` an.**

   Informationen zur Syntax des Befehls `netstat` finden Sie unter „Überwachen des Netzwerkstatus mit dem Befehl `netstat`" auf Seite 225 und in der Manpage `netstat(1M)`.

3. **Überprüfen·Sie die `hosts`-Datenbank (und, unter Solaris 10 11/06 und früheren Releases, die `ipnodes`-Datenbank, wenn Sie IPv6 verwenden) um sicherzustellen, dass die Einträge korrekt und auf dem neuesten Stand sind.**

   Informationen zur `/etc/inet/hosts`-Datenbank finden Sie unter „`hosts`-Datenbank" auf Seite 255 und in der Manpage `hosts(4)` Informationen zur `/etc/inet/ipnodes`-Datenbank finden Sie unter „`ipnodes`-Datenbank" auf Seite 259 und in der Manpage `ipnodes(4)`.

4. **Wenn Sie das Reverse Address Resolution Protocol (RARP) ausführen, zeigen Sie die Ethernet-Adressen in der `ethers`-Datenbank an, um sicherzustellen, dass die Einträge korrekt und auf dem neuesten Stand sind.**

5. **Versuchen Sie, mit dem Befehl `telnet` eine Verbindung zum lokalen Host herzustellen.**

   Informationen zur Syntax des Befehls `telnet` finden Sie in der Manpage `telnet(1)`.

6. **Stellen Sie sicher, dass der Netzwerk-Daemon `inetd` ausgeführt wird.**

   ```
   # ps -ef | grep inetd
   ```

   Die folgende Ausgabe bestätigt, dass der `inetd`-Daemon ausgeführt wird:

   ```
   root 57 1 0 Apr 04 ? 3:19 /usr/sbin/inetd -s
   ```

7 **Falls IPv6 in Ihrem Netzwerk aktiviert ist, prüfen Sie, ob der IPv6-Daemon `in.ndpd` ausgeführt wird:**

```
# ps -ef | grep in.ndpd
```

Die folgende Ausgabe bestätigt, dass der `in.ndpd`-Daemon ausgeführt wird:

```
root 123  1 0  Oct 27 ?  0:03 /usr/lib/inet/in.ndpd
```

Allgemeine Probleme bei der Bereitstellung von IPv6

In diesem Abschnitt werden die Fehler und Probleme beschrieben, die bei der Planung und Bereitstellung von IPv6 an Ihrem Standort auftreten könnten. Eine Liste der Planungsaufgaben finden Sie in Kapitel 4, „Planen eines IPv6-Netzwerks (Aufgaben)“.

IPv4-Router kann nicht auf IPv6 aufgerüstet werden

Falls Ihre bestehende Ausrüstung nicht aufgerüstet werden kann, müssen Sie eventuell eine IPv6-konforme Ausrüstung erwerben. Suchen Sie in der Dokumentation des Herstellers nach Verfahren, die Sie zur Unterstützung von IPv6 ausführen müssen.

Bestimmte IPv4-Router können nicht zur Unterstützung von IPv6 aufgerüstet werden. Falls dies auf Ihre Topologie zutrifft, verbinden Sie einen IPv6-Router mit einem IPv4-Router. Dann können Sie einen Tunnel vom IPv6-Router über den IPv4-Router konfigurieren. Informationen zu den Aufgaben beim Konfigurieren von Tunneln finden Sie unter „Aufgaben bei der Konfiguration von Tunneln zur Unterstützung von IPv6 (Übersicht der Schritte)“ auf Seite 204.

Probleme beim Aufrüsten von Services auf IPv6

Bei der Vorbereitung von Services zur Unterstützung von IPv6 tritt eventuell Folgendes auf:

- Einige Anwendungen aktivieren standardmäßig keine IPv6-Unterstützung, auch dann nicht, nachdem sie zu IPv6 portiert wurden. Eventuell müssen Sie diese Anwendungen konfigurieren, um IPv6 zu aktivieren.
- Auf einem Server, der mehrere Services ausführt, von denen einige ausschließlich IPv4-konform sind, andere sowohl IPv4 als auch IPv6 unterstützen, könnten Probleme auftreten. Einige Clients müssen beide Servicetypen unterstützen, was zu Fehlern auf dem Server führen kann.

Der aktuelle ISP unterstützt IPv6 nicht

Wenn Sie IPv6 bereitstellen möchten, Ihr aktueller ISP jedoch keine IPv6-Adressierung anbietet, sind neben dem ISP-Wechsel folgende Alternativen möglich:

- Beauftragen Sie einen ISP, eine zweite Leitung für IPv6-Kommunikationen von Ihrem Standort bereitzustellen. Diese Lösung ist kostenintensiv.
- Konfigurieren Sie einen *virtuellen ISP*. Ein virtueller ISP bietet Ihrem Standort IPv6-Konnektivität ohne einen Link. Stattdessen erstellen Sie einen Tunnel von Ihrem Standort über Ihren IPv4-ISP zum virtuellen ISP.
- Verwenden Sie einen 6to4-Tunnel über Ihren ISP zu anderen IPv6-Standorten. Bei der Adresse verwenden Sie die registrierte IPv4-Adresse des 6to4-Routers als öffentliche Topologiekomponente der IPv6-Adresse.

Sicherheitsbetrachtungen beim Tunneling zu einem 6to4-Relay-Router

Grundsätzlich ist ein Tunnel zwischen einem 6to4-Router und einem 6to4-Relay-Router unsicher. Sicherheitsprobleme wie die Folgenden tauchen bei Tunneln immer auf:

- Obwohl 6to4-Relay-Router Pakete einkapseln und entkapseln, prüfen dem Router keine der in den Paketen enthaltenen Daten.
- Adressen-Spoofing ist ein wesentliches Problem bei Tunneln zu einem 6to4-Relay-Router. Bei eingehenden Verkehr ist der 6to4-Router nicht in der Lage, die IPv4-Adresse des Relay-Routers mit der IPv6-Adresse der Quelle in Einklang zu bringen. Aus diesem Grund kann für die Adresse des IPv6-Hosts leicht ein Spoofing durchgeführt werden. Auch die Adresse des 6to4-Relay-Routers bietet ein Spoofing-Ziel.
- Standardmäßig existieren keine Vertrauensmechanismen zwischen 6to4-Routern und 6to4-Relay-Routern. Aus diesem Grund kann ein 6to4-Router nicht feststellen, ob der 6to4-Relay-Router vertrauenswürdig ist und ob es sich überhaupt um einen legitimen 6to4-Relay-Router handelt. Es muss eine vertrauenswürdige Beziehung zwischen 6to4-Standort und IPv6-Ziel bestehen, oder beide Standorte sind möglichen Angriffen offen ausgesetzt.

Diese und andere Sicherheitsprobleme im Zusammenhang mit 6to4-Relay-Routern sind im Internet Draft, *Security Considerations for 6to4* beschrieben. Allgemein sollten Sie die Unterstützung für 6to4-Relay-Router nur aus den folgenden Gründen aktivieren:

- Jeder 6to4-Standort muss mit einem privaten, vertrauenswürdigen IPv6-Netzwerk kommunizieren. Beispielsweise können Sie die Unterstützung eines 6to4-Relay-Routers in einem Universitätsnetzwerk aktivieren, das aus isolierten 6to4-Standorten und nativen IPv6-Standorten besteht.
- Ihr 6to4-Standort muss aus zwingenden geschäftlichen Gründen mit bestimmten nativen IPv6-Hosts kommunizieren.
- Sie haben die Prüfungs- und Vertrauensmodelle implementiert, die in der Internet Draft *Security Considerations for 6to4* vorgeschlagen werden.

Bekannte Probleme bei einem 6to4-Router

Die folgenden bekannten Programmfehler wirken sich auf die 6to4-Konfiguration aus:

- 4709338 – RIPng-Implementierung erforderlich, die statische Routen erkennt
- 4152864 – Konfiguration zweier Tunnel mit dem gleichen tsrc/tdst-Paar ist möglich

Implementierung statischer Routen an einem 6to4-Standort (Bug-ID 4709338)

Das folgende Problem tritt bei 6to4-Standorten mit Routern auf, die sich innerhalb des 6to4-Grenzrouters befinden. Wenn Sie die 6to4-Pseudoschnittstelle konfigurieren, wird die statische Route `2002::/16` automatisch zur Routing-Tabelle auf dem 6to4-Router hinzugefügt. Bug 4709338 beschreibt eine Einschränkung des Oracle Solaris RIPng-Routing-Protokolls, das verhindert, dass diese statische Route am 6to4-Standort bekannt gegeben wird.

Eine der folgenden Problemumgehungen ist für Bug 4709338 möglich.

- Fügen Sie die statische Route `2002::/16` den Routing-Tabellen aller Intrasite-Router am 6to4-Standort hinzu.
- Verwenden Sie ein anderes Protokoll als RIPng auf dem internen Router des 6to4-Standorts.

Konfiguration von Tunneln mit der gleichen Quelladresse (Bug-ID 4152864)

Bug-ID 4152864 beschreibt Probleme, die auftreten, wenn zwei Tunnel mit der gleichen Tunnel-Quelladresse konfiguriert wurden. Dies ist ein schwerwiegendes Problem bei 6to4-Tunneln.

Achtung – Konfigurieren Sie einen 6to4-Tunnel und einen automatischen Tunnel (`atun`) nicht mit der gleichen Tunnel-Quelladresse. Informationen zu automatischen Tunneln und dem Befehl `atun` finden Sie in der Manpage `tun(7M)`.

KAPITEL 10

TCP/IP und IPv4 im Detail (Referenz)

Dieses Kapitel enthält TCP/IP-Netzwerkreferenzen zu den Netzwerkkonfigurationsdateien, einschließlich Typ, Zweck und Format der Dateieinträge. Darüber hinaus werden die bestehenden Netzwerkdatenbanken detailliert beschrieben. Weiterhin zeigt das Kapitel, wie die Struktur der IPv4-Adressen basierend auf den Netzwerkklassifikationen und den Teilnetznummern abgeleitet wird.

Dieses Kapitel enthält die folgenden Informationen:

- „TCP/IP-Konfigurationsdateien“ auf Seite 253
- „Netzwerkdatenbanken und die `nsswitch.conf`-Datei“ auf Seite 264
- „Routing-Protokolle in Oracle Solaris“ auf Seite 273
- „Netzwerkklassen“ auf Seite 274

Neuerungen in diesem Kapitel

Unter Solaris 10 7/07 wird die `/etc/inet/ipnodes`-Datei nicht mehr benötigt. Verwenden Sie `/etc/inet/ipnodes` nur für frühere Oracle Solaris 10-Versionen, wie es in den jeweiligen Verfahren beschrieben wird.

TCP/IP-Konfigurationsdateien

Jedes System im Netzwerk bezieht die TCP/IP-Konfigurationsinformationen aus den folgenden TCP/IP-Konfigurationsdateien und Netzwerkdatenbanken:

- `/etc/hostname.`*Schnittstelle*-Datei
- `/etc/nodename`-Datei
- `/etc/defaultdomain`-Datei
- `/etc/defaultrouter`-Datei (optional)
- `hosts`-Datenbank
- Unter Solaris 10 11/06 und früheren Releases, `ipnodes`-Datenbank

- netmasks-Datenbank (optional)

Diese Dateien werden während der Installation vom Oracle Solaris-Installationsprogramm angelegt. Sie können diese Dateien gemäß den Anweisungen in diesem Abschnitt auch manuell bearbeiten. Die Datenbanken hosts und netmasks sind zwei der Netzwerkdatenbanken, die von den Namen-Services in Oracle Solaris-Netzwerken eingelesen werden. „Netzwerkdatenbanken und die nsswitch.conf-Datei" auf Seite 264 beschreibt das Konzept der Netzwerkdatenbanken ausführlich. Wenn Sie unter Solaris 10 11/06 oder früheren Releases arbeiten, finden Sie Informationen zur ipnodes-Datei unter „ipnodes-Datenbank" auf Seite 259.

/etc/hostname.*Schnittstelle*-Datei

Diese Datei definiert die physikalischen Netzwerkschnittstellen auf dem lokalen Host. Mindestens eine /etc/hostname.*Schnittstelle*-Datei sollte auf dem lokalen System vorhanden sein. Das Oracle Solaris-Installationsprogramm erstellt eine /etc/hostname.*Schnittstelle*-Datei für die erste während des Installationsprozesses erfasste Schnittstelle. Diese Schnittstelle hat in der Regel die niedrigste Gerätenummer, z. B. eri0, und wird als *primäre Netzwerkschnittstelle* bezeichnet. Erfasst das Installationsprogramm noch weitere Schnittstellen, können diese ebenfalls im Rahmen der Installation konfiguriert werden.

Hinweis – Wenn Sie alternative Hostname-Dateien für die gleiche Schnittstelle erstellen, müssen die alternativen Dateien ebenfalls dem Benennungsformathostname folgen.[0–9]*, wie z. B. hostname.qfe0.a123. Namen wiehostname.qfe0.bak oder hostname.qfe0.old sind ungültig und werden von Skripten beim Booten des Systems ignoriert.

Beachten Sie außerdem, dass eine angegebene Schnittstelle nur eine entsprechende Hostname-Datei haben darf. Wenn Sie eine alternative Hostname-Datei für eine Schnittstelle mit einem gültigen Dateinamen angeben, wie beispielsweise /etc/hostname.qfe und /etc/hostname.qfe.a123 , versuchen die Boot-Skripten, die Konfiguration durchzuführen, indem sie die Inhalte beider Hostname-Dateien referenzieren, woraus Fehler resultieren würden. Um diese Fehler zu vermeiden, geben Sie einen ungültigen Dateinamen für die Hostname-Datei an, die Sie in einer bestimmten Konfiguration nicht verwenden möchten.

Fügen Sie nach der Installation neue Netzwerkschnittstellen zu Ihrem System hinzu, wenn müssen Sie für diese Schnittstellen eine /etc/hostname.*Schnittstelle*-Datei erstellen. Dies wird unter „So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation" auf Seite 159 beschrieben. Damit Oracle Solaris die neue Netzwerkschnittstelle erkennt und verwendet, müssen Sie dem Gerätetreiber der Schnittstelle in das entsprechende Verzeichnis kopieren. Informationen zum geeigneten *Schnittstellen*namen und dem Gerätetreiber finden Sie in der Dokumentation der neuen Netzwerkschnittstelle.

Eine einfache `/etc/hostname.`*Schnittstelle*-Datei enthält nur einen Eintrag: den Hostnamen oder die IPv4-Adresse, der/die der Netzwerkschnittstelle zugeordnet ist. Die IPv4-Adresse kann im traditionellen getrennten dezimalen Format oder in der CIDR-Notation angegeben werden. Wenn Sie einen Hostnamen als Eintrag für die `/etc/hostname.`*Schnittstelle*-Datei verwenden, muss dieser Hostname auch in der `/etc/inet/hosts`-Datei vorhanden sein.

Angenommen, `smc0` ist die primäre Netzwerkschnittstelle für ein System mit der Bezeichnung `tenere`. Die Datei `/etc/hostname.smc0` kann entweder die IPv4-Adresse im getrennten dezimalen Format oder in der CIDR-Notation oder den Hostnamen `tenere` als Eintrag enthalten.

Hinweis – IPv6 verwendet die `/etc/hostname6.`*Schnittstelle*-Datei zur Definition von Netzwerkschnittstellen. Weitere Informationen hierzu finden Sie unter „IPv6-Schnittstellenkonfigurationsdatei“ auf Seite 288.

`/etc/nodename`-Datei

Diese Datei sollte nur einen Eintrag enthalten: den Hostnamen des lokalen Systems. Bei dem System `timbuktu` würde die Datei `/etc/nodename` nur den Eintrag `timbuktu` enthalten.

`/etc/defaultdomain`-Datei

Diese Datei sollte nur einen Eintrag enthalten: den vollständig qualifizierten Namen der administrativen Domäne, zu der das Netzwerk des lokalen Hosts gehört. Sie können diesen Namen dem Oracle Solaris-Installationsprogramm bereitstellen oder die Datei zu einem späteren Zeitpunkt bearbeiten. Weitere Informationen zu Netzwerkdomänen finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

`/etc/defaultrouter`-Datei

Diese Datei kann einen Eintrag für jeden Router enthalten, der direkt mit dem Netzwerk verbunden ist. Der Eintrag sollte der Name der Netzwerkschnittstelle sein, die als Router zwischen Netzwerken fungiert. Das Vorhandensein der `/etc/defaultrouter`-Datei kennzeichnet, dass das System zur Unterstützung des statischen Routings konfiguriert wurde.

`hosts`-Datenbank

Die `hosts`-Datenbank enthält die IPv4-Adressen und die Hostnamen der Systeme in Ihrem Netzwerk. Wenn Sie den Namen-Service NIS oder DNS oder den LDAP-Verzeichnisdienst

verwenden, wird die hosts-Datenbank in einer Datenbank verwaltet, die für Host-Informationen ausgelegt ist. In einem Netzwerk, das NIS ausführt, wird die hosts-Datenbank beispielsweise in der hostsbyname-Datei verwaltet.

Wenn Sie lokale Dateien als Namen-Service verwenden, wird die Datenbank hosts in der Datei /etc/inet/hosts verwaltet. Diese Datei enthält die Hostnamen und die IPv4-Adressen der primären Netzwerkschnittstelle, andere Netzwerkschnittstellen, die an das System angehängt sind und alle sonstigen Netzwerkadressen, die das System prüfen muss.

Hinweis – Um die Kompatibilität mit BSD-basierten Betriebssystemen aufrechtzuerhalten, stellt die /etc/hosts-Datei eine symbolische Verknüpfung zur /etc/inet/hosts-Datei dar.

/etc/inet/hosts-Dateiformat

Die Datei /etc/inet/hosts verwendet die folgende allgemeine Syntax. Vollständige Informationen zur Syntax finden Sie in der Manpage hosts(4).

IPv4-Adresse Hostname [Nicknamen] [#Kommentar]

IPv4-Adresse Enthält die IPv4-Adresse jeder Schnittstelle, die der lokalen Host erkennen muss.

Host-Name Enthält den Hostnamen, der dem System beim Setup zugewiesen wurde, sowie die Hostnamen, die zusätzlichen Netzwerkschnittstellen zugewiesen wurden und die dem lokalen Host bekannt sein müssen.

[Nickname] Ein optionales Feld, das einen Nicknamen für den Host enthält.

[#Kommentar] Ein optionales Feld für einen Kommentar.

Ursprüngliche /etc/inet/hosts-Datei

Wenn Sie das Oracle Solaris-Installationsprogramm auf einem System ausführen, konfiguriert das Programm eine ursprüngliche /etc/inet/hosts-Datei. Diese Datei enthält die Mindestanzahl an Einträgen, die für den lokalen Host erforderlich sind. Diese Einträge umfassen die Loopback-Adresse, die IPv4-Adresse des Hosts und den Hostnamen.

Angenommen, das Oracle Solaris-Installationsprogramm erstellt die folgende /etc/inet/hosts-Datei für das System tenere, das in Abbildung 5–1 vorgestellt wurde:

BEISPIEL 10–1 /etc/inet/hosts-Datei für das System tenere

```
127.0.0.1     localhost         loghost    #loopback address
192.168.200.3   tenere                      #host name
```

Loopback-Adresse

In Beispiel 10–1 ist die IPv4-Adresse `127.0.0.1` die *Loopback-Adresse*. Die Loopback-Adresse ist eine reservierte Netzwerkschnittstelle, die vom lokalen System für eine prozessinterne Konfiguration verwendet wird. Über diese Adresse kann der Host Pakete an sich selbst senden. Der Befehl `ifconfig` verwendet die Loopback-Adresse zur Konfiguration und zu Testzwecken. Dies wird unter „Überwachen der Schnittstellenkonfiguration mit dem Befehl `ifconfig`“ auf Seite 221 beschrieben. Jedes System in einem TCP/IP-Netzwerk muss die IP-Adresse `127.0.0.1` als IPv4-Loopback auf dem lokalen Host verwenden.

Hostname

Die IPv4-Adresse `192.168.200.1` und der Name `tenere` sind die Adresse und der Hostname des lokalen Systems. Sie sind der primären Netzwerkschnittstelle des Systems zugeordnet.

Mehrere Netzwerkschnittstellen

Einige Systeme verfügen über mehrere Netzwerkschnittstellen, da es sich entweder um Router oder um Multihomed-Hosts handelt. Jede an ein System angehängte Netzwerkschnittstelle benötigt eine eigene IP-Adresse sowie einen zugewiesenen Namen. Sie müssen während der Installation eine primäre Netzwerkschnittstelle konfigurieren. Verfügt ein bestimmtes System während der Installation über mehrere Schnittstellen, fordert Sie das Oracle Solaris-Installationsprogramm auf, diese zusätzlichen Schnittstellen zu konfigurieren. Sie können diese zusätzlichen Schnittstellen entweder während der Installation oder zu einem späteren Zeitpunkt manuell konfigurieren.

Nach der Installation von Oracle Solaris können Sie zusätzliche Schnittstellen für einen Router oder einen Multihomed-Host konfigurieren, indem Sie die Schnittstelleninformationen einfach in die `/etc/inet/hosts`-Datei eingeben. Weitere Informationen zur Konfiguration von Routern und Multihomed-Hosts finden Sie unter „Konfiguration eines IPv4-Routers“ auf Seite 126 und „Konfiguration von Multihomed-Hosts“ auf Seite 134.

Beispiel 10–2 zeigt die `/etc/inet/hosts`-Datei für das System `timbuktu`, das in Abbildung 5–1 vorgestellt wurde.

BEISPIEL 10–2 `/etc/inet/hosts`-Datei für das System `timbuktu`

```
127.0.0.1        localhost     loghost
192.168.200.70   timbuktu      #This is the local host name
192.168.201.10   timbuktu-201  #Interface to network 192.9.201
```

Mit diesen beiden Schnittstellen kann `timbuktu` die beiden Netzwerke `192.168.200` und `192.168.201` als Router miteinander verbinden.

So wirken sich Namen-Services auf die `hosts`-Datenbank aus

Die Namen-Services NIS und DNS und der LDAP-Verzeichnisdienst verwalten die Hostnamen und Adressen entweder auf einem oder auf mehreren Servern. Diese Server pflegen `hosts`-Datenbanken, in denen Informationen zu den Hosts und Routern (sofern anwendbar) im Netzwerk des Servers gespeichert sind. Weitere Informationen zu diesen Services finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Wenn lokale Dateien den Namen-Service bereitstellen

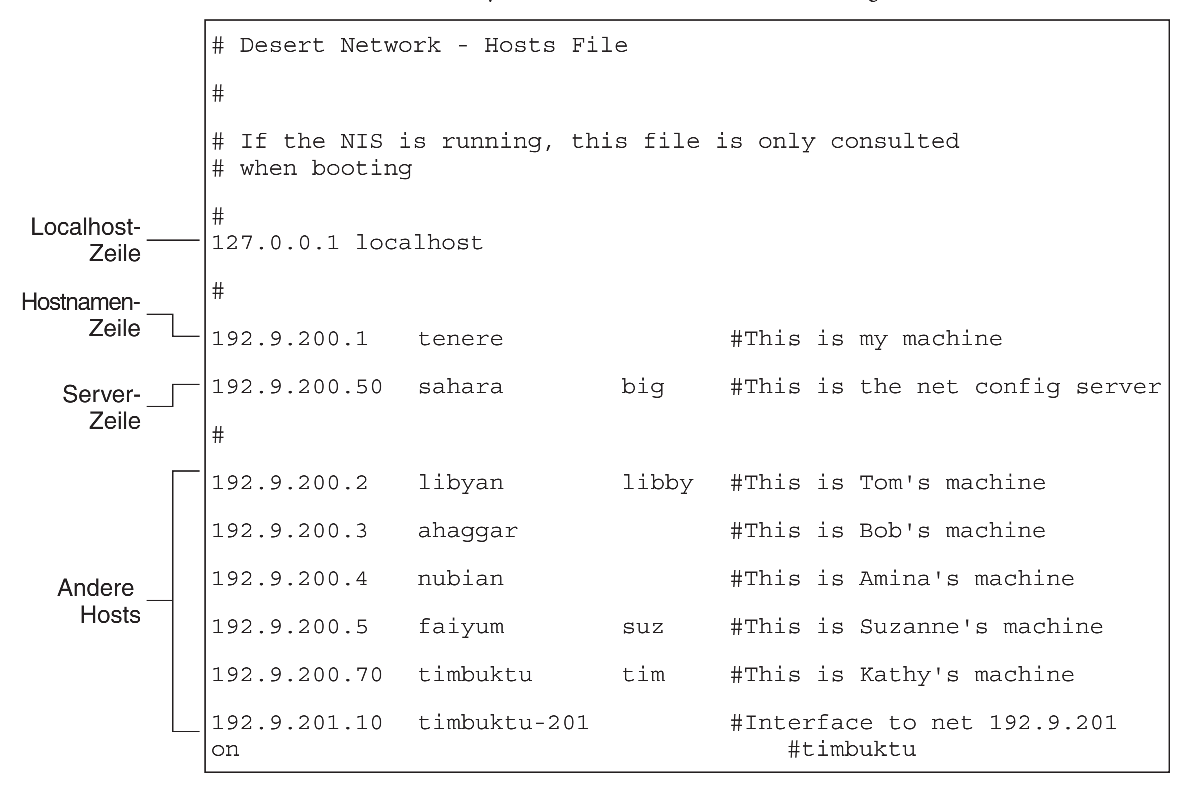
In einem Netzwerk, in dem lokale Dateien als Namen-Services dienen, verwenden Systeme im lokale Dateien-Modus ihre individuellen `/etc/inet/hosts`-Dateien, um Informationen zu den IPv4-Adressen und Hostnamen anderer Systeme im Netzwerk abzurufen. Aus diesem Grund müssen die `/etc/inet/hosts`-Dateien dieser Systeme Folgendes enthalten:

- Loopback-Adresse
- IPv4-Adresse und Hostname des lokalen Systems (primäre Netzwerkschnittstelle)
- IPv4-Adresse und Hostname der zusätzliche Netzwerkschnittstellen, die an dieses System angehängt sind (sofern anwendbar)
- IPv4-Adressen und Hostnamen aller Hosts im lokalen System
- IPv4-Adressen und Hostnamen aller Router, über die dieses System informiert sein muss (sofern anwendbar)
- IPv4-Adresse aller Systeme, die Ihr System über den Hostnamen anspricht

Abbildung 10–1 zeigt die `/etc/inet/hosts`-Datei für das System `tenere`. Dieses System wird im lokale Dateien-Modus ausgeführt. Beachten Sie, dass die Datei die IPv4-Adressen und Hostnamen jedes Systems im Netzwerk `192.9.200` enthält. Darüber hinaus enthält die Datei die IPv4-Adresse sowie den Schnittstellennamen `timbuktu-201`. Diese Schnittstelle verbindet das Netzwerk `192.9.200` mit dem Netzwerk `192.9.201`.

Ein als Netzwerkclient konfiguriertes System verwendet die lokale Datei `/etc/inet/hosts` für seine Loopback- und die IPv4-Adresse.

ABBILDUNG 10–1 `/etc/inet/hosts`-Datei für ein System, das im lokale Dateien-Modus ausgeführt wird




```
# Desert Network - Hosts File
#
# If the NIS is running, this file is only consulted
# when booting
#
127.0.0.1 localhost
#
192.9.200.1    tenere                 #This is my machine
192.9.200.50   sahara        big      #This is the net config server
#
192.9.200.2    libyan        libby    #This is Tom's machine
192.9.200.3    ahaggar                #This is Bob's machine
192.9.200.4    nubian                 #This is Amina's machine
192.9.200.5    faiyum        suz      #This is Suzanne's machine
192.9.200.70   timbuktu      tim      #This is Kathy's machine
192.9.201.10   timbuktu-201           #Interface to net 192.9.201
on                                        #timbuktu
```

`ipnodes`-Datenbank

Hinweis – Die `ipnodes`-Datenbank ist in Releases nach Solaris 10 11/06 nicht mehr enthalten. In den nachfolgenden Releases sind die IPv6-Funktionen der `ipnodes`-Datenbank in die `hosts`-Datenbank eingeflossen.

Die `/etc/inet/ipnodes`-Datei nimmt sowohl IPv4 -als auch IPv6-Adressen auf. Die IPv4-Adressen können entweder im traditionellen getrennten dezimalen Format oder in der CIDR-Notation gespeichert werden. Diese Datei dient als eine lokale Datenbank, die Hostnamen mit den zugehörigen IPv4- und IPv6-Adressen verknüpft. Speichern Sie Hostnamen und deren Adressen nicht in statischen Dateien wie `/etc/inet/ipnodes`. Speichern Sie die IPv6-Adressen zu Testzwecken auf die gleiche Weise, wie IPv4-Adressen in `/etc/inet/hosts` gespeichert werden. Die `ipnodes`-Datei verwendet die gleichen Formatskonventionen wie die `hosts`-Datei. Weitere Informationen zur `/etc/inet/hosts`-Datei finden Sie unter „`hosts`-Datenbank" auf Seite 255. Eine Beschreibung der `ipnodes`-Datei finden Sie in der Manpage `ipnodes(4)`.

IPv6-konforme Anwendungen verwenden die `/etc/inet/ipnodes`-Datenbank. Die bestehende `/etc/hosts`-Datenbank, in der nur IPv4-Adressen enthalten sind, bleibt gleich, um das Arbeiten mit vorhandenen Anwendungen zu vereinfachen. Wenn die `ipnodes`-Datenbank nicht existiert, verwenden IPv6-konforme Anwendungen die vorhandene `hosts`-Datenbank.

Hinweis – Wenn Sie Adressen hinzufügen müssen, fügen Sie die IPv4-Adressen der `hosts`- und der `ipnodes`-Datei hinzu. IPv6-Adressen werden nur der `ipnodes`-Datei hinzugefügt.

BEISPIEL 10–3 `/etc/inet/ipnodes`-Datei

Hostnamenadressen müssen nach dem Hostnamen gruppiert werden. Dies wird in dem folgenden Beispiel gezeigt.

```
#
# Internet IPv6 host table
# with both IPv4 and IPv6 addresses
#
::1     localhost
2001:db8:3b4c:114:a00:20ff:fe78:f37c   farsite.com farsite farsite-v6
fe80::a00:20ff:fe78:f37c     farsite-11.com farsitell
192.168.85.87                    farsite.com farsite farsite-v4
2001:db8:86c0:32:a00:20ff:fe87:9aba   nearsite.com nearsite nearsite-v6
fe80::a00:20ff:fe87:9aba     nearsite-11.com nearsitell
10.0.0.177                   nearsite.com nearsite nearsite-v4 loghost
```

`netmasks`-Datenbank

Die `netmasks`-Datenbank muss *nur* dann im Rahmen der Netzwerkkonfiguration bearbeitet werden, wenn Sie Teilnetze für Ihr Netzwerk eingerichtet haben. Die `netmasks`-Datenbank enthält eine Liste der Netzwerke und deren zugewiesenen Teilnetzmasken.

Hinweis – Wenn Sie Teilnetze erstellen, muss jedes neue Netzwerk ein separates physikalisches Netzwerk sein. Teilnetze können nicht in einem einzelnen physikalischen Netzwerk eingerichtet werden.

Was versteht man unter Subnetting?

Subnetting ist eine Methode zur Maximierung des eingeschränkten 32-Bit-IPv4-Adressraums, während gleichzeitig die Größe der Routing-Tabellen in einem großen Internetzwerk reduziert wird. Subnetting bietet bei allen Adressklassen eine Möglichkeit, einen Teil des Host-Adressraums so Netzwerkadressen zugeordnet wird, dass Sie mehr Netzwerke erhalten. Die Komponente des Host-Adressraums, der die neuen Netzwerkadressen zugeordnet werden, wird als *Teilnetznummer* bezeichnet.

Neben der effizienteren Nutzung des IPv4-Adressraums bietet das Subnetting verschiedene administrative Vorteile. Mit steigender Anzahl an Netzwerken wird das Routing sehr komplex. Ein kleines Unternehmen kann jedem lokalen Netzwerk z. B. eine Klasse-C-Nummer zuordnen. Wenn das Unternehmen wächst, wird die Verwaltung verschiedener Netzwerknummern immer komplizierter. Besser ist es, jeder wichtigen Abteilung in einem Unternehmen einige wenige Klasse-B-Netzwerknummern zuzuweisen. Beispielsweise können Sie ein Klasse-B-Netzwerk für die Technikabteilung, ein Klasse-B-Netzwerk für die Betriebsabteilung usw. zuweisen. Dann können Sie jedes Klasse-B-Netzwerk in weitere Netzwerke unterteilen und dabei die zusätzlichen Netzwerknummern nutzen, die durch das Subnetting erhalten werden. Diese Aufteilung reduziert auch die Routing-Informationen, die zwischen Routern übertragen werden müssen.

Erstellen der Netzwerkmaske für IPv4-Adressen

Im Rahmen des Subnetting-Prozesses müssen Sie eine im gesamten Netzwerk gültige *Netzmaske* auswählen. Die Netzmaske legt fest, wie viele und welche Bit im Host-Adressraum die Teilnetznummer darstellen und wie viele und welche Bit für die Hostnummer stehen. Sie erinnern sich, eine vollständige IPv4-Adresse besteht aus 32 Bit. Abhängig von der Adressklasse stehen bis zu 24 Bit oder nur 8 Bit für die Darstellung des Host-Adressraums zur Verfügung. Die Netzmaske wird in der `netmasks`-Datenbank angegeben.

Wenn Sie beabsichtigen, Teilnetze einzusetzen, müssen Sie Ihre Netzmaske vor der Konfiguration von TCP/IP festlegen. Möchten Sie das Betriebssystem im Rahmen der Netzwerkkonfiguration installieren, fordert das Oracle Solaris-Installationsprogramm die Netzmaske für Ihr Netzwerk an.

Wie unter „Erstellen eines IPv4-Adressierungsschemas“ auf Seite 61 beschrieben, bestehen 32-Bit-IP-Adressen aus einer Netzwerk- und einer Hostkomponente. Die 32 Bit werden in 4 Byte unterteilt. Jedes Byte ist, abhängig von der Netzwerkklasse, entweder der Netzwerknummer oder der Hostnummer zugeordnet.

Bei einer Klasse-B-IPv4-Adresse sind die 2 Byte auf der linken Seite der Netzwerknummer und die 2 Byte auf der rechten Seite der Hostnummer zugeordnet. Bei der Klasse-B-IPv4-Adresse `172.16.10` können Sie die 2 Byte auf der rechten Seite Hosts zuweisen.

Wenn Sie das Subnetting implementieren, benötigen Sie einige Bit im Byte der Hostnummer für die Teilnetzadressen. Beispielsweise bietet ein 16-Bit-Host-Adressraum Adressen für 65.534 Hosts. Wenn Sie das dritte Byte für Teilnetzadressen und das vierte Byte für Hostadressen verwenden, können Sie bis zu 254 Netzwerke mit jeweils bis zu 254 Hosts adressieren.

Die Bit in den Hostadressen-Byte für Teilnetzadresse und die Bit für Hostadressen werden durch eine *Teilnetzmaske* festgelegt. Teilnetzmasken dienen zur Auswahl der Bit von beiden Byte für die Verwendung als Teilnetzadresse. Obwohl die Netzmaskenbit aufeinander folgend sein müssen, müssen sie nicht in Byte-Segmenten ausgerichtet sein.

Die Netzmaske kann mithilfe des bitweise logischen UND-Operators an einer IPv4-Adresse angewendet werden. Dieser Vorgang wählt die Positionen der Netzwerknummer und der Teilnetznummer in der Adresse.

Netzmasken können über ihre Binärdarstellung erklärt werden. Zur Binär-Dezimal-Umwandlung können Sie einen Taschenrechner verwenden. Die folgenden Beispiele zeigen sowohl die dezimalen als auch die binären Formen der Netzmaske.

Wenn die Netzmaske `255.255.255.0` an der IPv4-Adresse `172.16.41.101` angewendet wird, ist das Ergebnis die IPv4-Adresse `172.16.41.0`.

`172.16.41.101` & `255.255.255.0` = `172.16.41.0`

In binärer Form läuft der Vorgang wie folgt ab:

10000001.10010000.00101001.01100101 (IPv4-Adresse)

AND-Vorgang mit

11111111.11111111.11111111.00000000 (Netzmaske)

Jetzt sucht das System nach der Netzwerknummer `172.16.41` anstatt nach der Netzwerknummer `172.16`. Ist die Adresse `172.16.41` in Ihrem Netzwerk vorhanden, ist diese Adresse diejenige, die das System sucht und findet. Da Sie dem dritten Byte des IPv4-Adressraums bis zu 254 Werte zuweisen können, können Sie durch Subnetting Adressraum für 254 Netzwerke erstellen, während vorher nur eines verfügbar war.

Wenn Sie nur für zwei zusätzliche Netzwerke Adressraum bereitstellen, können Sie die folgende Teilnetzmaske verwenden:

`255.255.192.0`

Diese Netzmaske bietet das folgende Ergebnis:

11111111.11111111.1100000.00000000

Bei diesem Ergebnis verbleiben noch 14 Bit für Hostadressen. Da alle 0en und 1en reserviert sind, müssen mindestens zwei Bit für die Hostnummer reserviert werden.

`/etc/inet/netmasks`-Datei

Wenn Ihr Netzwerk NIS oder LDAP ausführt, pflegen die Server `netmasks`-Datenbanken für diese Namen-Services. Bei Netzwerken, die lokale Dateien als Namen-Service verwenden, werden diese Informationen in der `/etc/inet/netmasks`-Datei gepflegt.

Hinweis – Um die Kompatibilität mit BSD-basierten Betriebssystemen aufrechtzuerhalten , ist die `/etc/netmasks`-Datei eine symbolische Verknüpfung zur `/etc/inet/netmasks`-Datei.

Das folgende Beispiel zeigt die `/etc/inet/netmasks`-Datei für ein Klasse-B-Netzwerk.

BEISPIEL 10–4 `/etc/inet/netmasks`-Datei für ein Klasse-B-Netzwerk

```
# The netmasks file associates Internet Protocol (IPv4) address
# masks with IPv4 network numbers.
#
#     network-number    netmask
#
# Both the network-number and the netmasks are specified in
# “decimal dot” notation, e.g:
#
#        128.32.0.0   255.255.255.0
192.168.0.0  255.255.255.0
```

Wenn die Datei `/etc/netmasks` nicht vorhanden ist, muss sie mit einem Texteditor erstellt werden. Verwenden Sie die folgende Syntax:

network-number   netmask-number

Ausführliche Informationen finden Sie in der Manpage `netmasks(4)`.

Beim Erstellen der Netzmaskennummern geben Sie die vom ISP oder der Internet Registry zugewiesene Netzwerknummer (nicht die Teilnetznummer) und die Netzmaskennummer in die `/etc/inet/netmasks`-Datei ein. Jede Teilnetzmaske muss auf einer separaten Zeile erscheinen.

Beispiel:

```
128.78.0.0        255.255.248.0
```

Sie können auch symbolische Namen für die Netzwerknummern in die `/etc/inet/hosts`-Datei eingeben. Dann verwenden Sie diese Netzwerknamen anstelle der Netzwerknummern als Parameter für Befehle.

`inetd` Internet Services-Daemon

Der `inetd`-Daemon startet die standardmäßigen Internet Services beim Booten eines Systems und kann einen Service bei aktivem System neustarten. Mit dem Service Management Facility (SMF) können Sie standardmäßige Internet Services bearbeiten oder zusätzliche Services durch den `inetd`-Daemon starten.

Mit dem folgenden SMF-Befehlen können Sie Services verwalten, die von inetd-Daemon gestartet wurden:

svcadm
: Für administrative Aktionen an einem Service, z. B. Aktivieren, Deaktivieren oder Neustarten. Ausführliche Informationen finden Sie in der Manpage svcadm(1M).

svcs
: Zum Abfragen des Status eines Services. Ausführliche Informationen finden Sie in der Manpage svcs(1).

inetadm
: Zum Anzeigen und Bearbeiten der Eigenschaften eines Services. Ausführliche Informationen finden Sie in der Manpage inetadm(1M).

Der Feldwert proto im inetadm-Profil eines bestimmten Services gibt das Transportschichtprotokoll an, auf dem der Service ausgeführt wird. Wenn der Service nur IPv4-konform ist, muss in dem Feld proto entweder tcp, udp oder sctp angegeben werden.

- Anweisungen zum Verwenden der SMF-Befehle finden Sie im „SMF Command-Line Administrative Utilities“ in *System Administration Guide: Basic Administration*.
- Eine Beispielaufgabe, in der SMF-Befehle zum Hinzufügen eines über SCTP ausgeführten Services verwendet werden, finden Sie unter „So fügen Sie Services hinzu, die das SCTP-Protokoll verwenden“ auf Seite 143.
- Informationen zum Hinzufügen von Services, die sowohl IPv4- als auch IPv6-Anforderungen verarbeiten können, finden Sie unter „inetd Internet Services-Daemon“ auf Seite 263

Netzwerkdatenbanken und die nsswitch.conf-Datei

Netzwerkdatenbanken sind Dateien, die für die Konfiguration des Netzwerks erforderliche Informationen bereitstellen. Folgende Netzwerkdatenbanken stehen zur Verfügung:

- hosts
- netmasks
- ethers
- bootparams
- protocols
- services
- networks

Wenn Ihr Netzwerk über Teilnetze verfügt, werden die Datenbanken hosts und netmasks im Rahmen der Konfiguration bearbeitet. Zwei Netzwerkdatenbanken , bootparams und ethers, dienen zur Konfiguration von Systemen als Netzwerkclients. Die verbleibenden Datenbanken werden vom Betriebssystem verwendet und müssen nur selten bearbeitet werden.

Obwohl es sich bei der Datei nsswitch.conf nicht um eine Netzwerkdatenbanken handelt, müssen Sie diese Datei zusammen mit den jeweiligen Netzwerkdatenbanken konfigurieren.

`nsswitch.conf gibt an, welcher Namen-Service für ein bestimmtes System verwendet wird: lokale Dateien, NIS, DNS oder LDAP.`

Auswirkungen der Namen-Services auf Netzwerkdatenbanken

Das Format Ihrer Netzwerkdatenbanken hängt vom Typ des Namen-Services ab, den Sie für Ihr Netzwerk auswählen. Beispielsweise enthält die `hosts`-Datenbank mindestens den Hostnamen und die IPv4-Adresse des lokalen Systems sowie alle Netzwerkschnittstellen, die direkt mit dem lokalen System verbunden sind. Darüber hinaus könnte die `hosts`-Datenbank, abhängig vom Typ des Namen-Services in Ihrem Netzwerk, noch weitere IPv4-Adressen und Hostnamen enthalten.

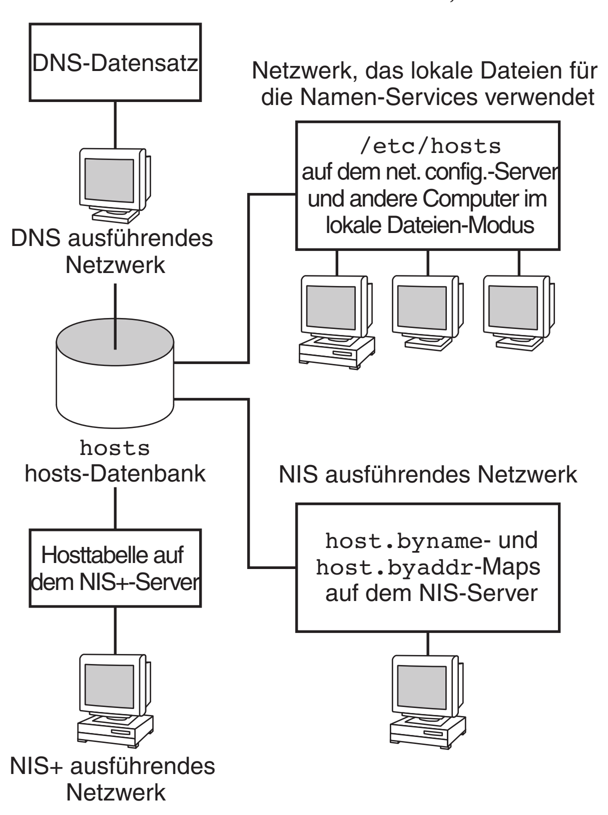
Die Netzwerkdatenbanken werden wie folgt verwendet:

- Netzwerke, die lokale Dateien als Namen-Service verwenden, beziehen ihre Informationen aus Dateien in den Verzeichnissen `/etc/inet` und `/etc`.
- NIS verwendet Datenbanken, die als NIS Maps bezeichnet werden.
- DNS verwendet Datensätze mit Hostinformationen.

Hinweis – DNS-Boot- und Datendateien entsprechen Netzwerkdatenbanken nicht direkt.

Die folgende Abbildung zeigt Formen der `hosts`-Datenbank, die von diesen Namen-Services verwendet werden.

ABBILDUNG 10–2 Formen der hosts-Datenbank, die von Namen-Services verwendet werden



In der folgenden Tabelle sind die Netzwerkdatenbanken sowie deren entsprechende lokale Dateien und NIS Maps aufgeführt.

Hinweis – Die ipnodes-Datenbank wurde in den Oracle Solaris-Versionen nach Solaris 10 11/06 entfernt.

TABELLE 10–1 Netzwerkdatenbanken und entsprechenden Namen-Service-Dateien

Netzwerkdatenbank	Lokale Dateien	NIS-Maps
hosts	/etc/inet/hosts	hosts.byaddr hosts.byname
ipnodes	/etc/inet/ipnodes	ipnodes.byaddr ipnodes.byname
netmasks	/etc/inet/netmasks	netmasks.byaddr
ethers	/etc/ethers	ethers.byname ethers.byaddr

TABELLE 10–1 Netzwerkdatenbanken und entsprechenden Namen-Service-Dateien *(Fortsetzung)*

Netzwerkdatenbank	Lokale Dateien	NIS-Maps
bootparams	/etc/bootparams	bootparams
protocols	/etc/inet/protocols	protocols.byname protocols.bynumber
services	/etc/inet/services	services.byname
networks	/etc/inet/networks	networks.byaddr networks.byname

In diesem Buch werden die Netzwerkdatenbanken beschrieben, wie sie von Netzwerken gesehen werden, die lokale Dateien als Namen-Service verwenden.

- Informationen zur hosts-Datenbank finden Sie unter „hosts-Datenbank“ auf Seite 255.
- Informationen zur netmasks-Datenbank finden Sie unter „netmasks-Datenbank“ auf Seite 260.
- Für Solaris 10 11/06 und frühere Releases finden Sie Informationen zur ipnodes-Datenbank unter „ipnodes-Datenbank“ auf Seite 259.

Informationen zu den Netzwerkdatenbank-Entsprechungen bei den Namen-Services NIS, DNS und LDAP finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

nsswitch.conf-Datei

Die Suchreihenfolge der Netzwerkdatenbanken wird in der Datei /etc/nsswitch.conf definiert. Das Oracle Solaris-Installationsprogramm erstellt eine standardmäßige /etc/nsswitch.conf-Datei für das lokale System, die auf dem Namen-Service basiert, den Sie während der Installation angegeben haben. Mit der Option „Keinen“ wählen Sie lokale Dateien als Namen-Service. Die resultierende nsswitch.conf-Datei sieht etwa wie folgt aus.

BEISPIEL 10–5 nsswitch.conf-Datei für Netzwerke, die lokale Dateien als Namen-Service verwenden

```
# /etc/nsswitch.files:
#
# An example file that could be copied over to /etc/nsswitch.conf;
# it does not use any naming service.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file contains "switch.so" as a
# nametoaddr library for "inet" transports.

passwd:         files
group:          files
hosts:          files
networks:       files
protocols:      files
rpc:            files
```

BEISPIEL 10–5 nsswitch.conf-Datei für Netzwerke, die lokale Dateien als Namen-Service verwenden *(Fortsetzung)*

```
ethers:         files
netmasks:       files
bootparams:     files
publickey:      files
# At present there isn't a 'files' backend for netgroup; the
# system will figure it out pretty quickly,
# and won't use netgroups at all.
netgroup:       files
automount:      files
aliases:        files
services:       files
sendmailvars:   files
```

Diese Datei wird ausführlich in der Manpage nsswitch.conf(4) beschrieben. Die allgemeine Syntax lautet:

Datenbank zu-durchsuchender-Namen-Service

Das Feld *Datenbank* kann einen der vielen Datenbanktypen enthalten, die das Betriebssystem durchsuchen kann. Beispielsweise könnte das Feld eine Datenbank angeben, die sich auf Benutzer auswirkt (z. B. passwd oder aliases), oder eine Netzwerkdatenbanken. Der Parameter *zu-durchsuchender-Namen-Service* kann die Werte files, nis oder nis+ für die Netzwerkdatenbanken annehmen. Die hosts-Datenbank kann auch dns als zu durchsuchenden Namen-Service enthalten. Sie können auch mehrere Namen-Services anführen, z. B. nis+ und files.

In Beispiel 10–5 ist die einzige angegebene Suchoption files. Aus diesem Grund bezieht das lokale System die Informationen zur Sicherheit und zum Automounting wie auch die Netzwerkdatenbank-Informationen aus Dateien, die sich in den Verzeichnissen /etc und /etc/inet befinden.

Ändern der Datei nsswitch.conf

Das Verzeichnis /etc enthält die vom Oracle Solaris-Installationsprogramm angelegte Datei nsswitch.conf. Darüber hinaus enthält dieses Verzeichnis die Vorlagendateien für die folgenden Namen-Services:

- nsswitch.files
- nsswitch.nis

Wenn Sie von einem Namen-Services zu einem anderen wechseln möchten, können Sie die entsprechende Vorlage in nsswitch.conf kopieren. Sie können nsswitch.conf auch selektiv bearbeiten und den standardmäßig zu durchsuchenden Namen-Service für einzelne Datenbanken ändern.

Angenommen, ein Netzwerk führt NIS aus, und Sie möchten die nsswitch.conf-Datei auf dem Netzwerkclients ändern. Der Suchpfad für die Datenbanken bootparams und ethers muss als erste Option files und dann nis enthalten. Das folgende Beispiel zeigt die korrekten Suchpfade.

BEISPIEL 10–6 nsswitch.conf-Datei für einen Client in einem Netzwerk, das NIS ausführt

```
# /etc/nsswitch.conf:#
.
.
passwd:        files nis
group:         files nis

# consult /etc "files" only if nis is down.
hosts:         nis    [NOTFOUND=return] files
networks:      nis    [NOTFOUND=return] files
protocols:     nis    [NOTFOUND=return] files
rpc:           nis    [NOTFOUND=return] files
ethers:        files  [NOTFOUND=return] nis
netmasks:      nis    [NOTFOUND=return] files
bootparams:    files  [NOTFOUND=return] nis
publickey:     nis
netgroup:      nis

automount:     files nis
aliases:       files nis

# for efficient getservbyname() avoid nis
services:      files nis
sendmailvars:  files
```

Ausführliche Informationen zum Ändern des Namen-Services finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

bootparams-Datenbank

Die bootparams-Datenbank enthält Informationen, die von Systemen genutzt werden, die im Netzwerkclient-Modus booten. Sie müssen diese Datenbank bearbeiten, falls Ihr Netzwerk über Netzwerkclients verfügt. Informationen zu den Verfahren finden Sie unter „Konfiguration der Netzwerkclients“ auf Seite 113 Die Datenbank wird aus den Informationen erstellt, die in die /etc/bootparams-Datei eingegeben wurde.

Vollständige Informationen zur Syntax für diese Datenbank finden Sie in der Manpage bootparams(4) Die allgemeine Syntax lautet:

Systemname Dateischlüssel-Servername:Pfadname

Ein Eintrag für ein Netzwerkclientsystem kann die folgenden Informationen umfassen: Name des Clients, eine Liste der Schlüssel, die Namen der Server und die Pfadnamen. Das erste Objekt jedes Eintrags ist der Name des Clientsystems. Alle Objekte außer dem ersten sind optional. Ein Beispiel:

BEISPIEL 10–7 bootparams-Datenbank

```
myclient   root=myserver : /nfsroot/myclient  \
swap=myserver : /nfsswap//myclient \
dump=myserver : /nfsdump/myclient
```

In diesem Beispiel weist der Begriff dump= Clienthosts an, nicht nach einer Dump-Datei zu suchen.

Platzhaltereintrag für bootparams

In den meisten Fällen verwenden Sie einen Platzhaltereintrag, wenn Sie die bootparams-Datenbank bearbeiten, um bestimmte Clients zu unterstützen. Ein Beispieleintrag:

```
*   root=server:/path dump=:
```

Der Platzhalter (*) gibt an, dass dieser Eintrag für alle Clients gilt, die nicht namentlich in der bootparams-Datenbank aufgeführt sind.

ethers-Datenbank

Die ethers-Datenbank wird aus den Informationen erstellt, die in die /etc/ethers-Datei eingegeben wurden. Diese Datenbank ordnet Hostnamen zu ihren *Media Access Control* (MAC)-Adressen zu. Sie müssen nur dann eine ethers-Datenbank erstellen, wenn Sie den RARP-Daemon ausführen. Das heißt, Sie müssen diese Datenbank erstellen, wenn Sie Netzwerkclients konfigurieren.

RARP ordnet mithilfe dieser Datei MAC-Adressen zu IP-Adressen zu. Wenn Sie den RARP-Daemon in.rarpd ausführen, müssen Sie die ethers-Datei einrichten und auf allen den Daemon ausführenden Hosts pflegen, um die Änderungen im Netzwerk widerzuspiegeln.

Vollständige Informationen zur Syntax für diese Datenbank finden Sie in der Manpage ethers(4) Die allgemeine Syntax lautet:

MAC-address   hostname   #comment

MAC-Adresse	Die MAC-Adresse des Hosts
Host-Name	Der offizielle Name des Hosts
#Kommentar	Ein Hinweis, der an einen Eintrag in der Datei angehängt werden soll

Die MAC-Adresse wird vom Gerätehersteller bereitgestellt. Wenn das System die MAC-Adresse während des Bootens nicht anzeigt, schlagen Sie in den Hardware-Handbüchern nach.

Stellen Sie beim Hinzufügen von Einträgen zur ethers-Datenbank sicher, dass die Hostnamen in der hosts-Datenbank (und, unter Solaris 10 11/06 und früheren Releases, in der ipnodes-Datenbank) den primären Namen und nicht den Nicknamen entsprechen.

BEISPIEL 10–8 Einträge in der ethers-Datenbank

```
8:0:20:1:40:16   fayoum
8:0:20:1:40:15   nubian
8:0:20:1:40:7    sahara    # This is a comment
8:0:20:1:40:14   tenere
```

Andere Netzwerkdatenbanken

Die übrigen Netzwerkdatenbanken müssen nur selten bearbeitet werden.

networks-Datenbank

Die networks-Datenbank ordnet Netzwerknummern den Netzwerknamen zu und ermöglicht bestimmten Anwendungen, Namen anstelle von Zahlen zu verwenden und anzuzeigen. Die networks-Datenbank basiert auf den Informationen in der /etc/inet/networks-Datei. Diese Datei enthält die Namen aller Netzwerke, mit denen Ihr Netzwerk über Router verbunden ist.

Das Oracle Solaris-Installationsprogramm konfiguriert eine erste networks-Datenbank. Wenn Sie jedoch Ihrer vorhandenen Netzwerktopologie ein neues Netzwerk hinzufügen, müssen Sie diese Datenbank aktualisieren.

Die Manpage networks(4) enthält ausführliche Informationen zur Syntax der /etc/inet/networks-Datei. Die allgemeine Syntax lautet:

network-name network-number nickname(s) #comment

Netzwerkname	Offizieller Name des Netzwerks
Netzwerknummer	Adresse, die vom ISP oder der Internet Registry zugewiesen wurde
Nickname	Ein weiterer Name, unter dem das Netzwerk bekannt ist
#Kommentar	Ein Hinweis, der an einen Eintrag in der Datei angehängt werden soll

Sie müssen die networks-Datei pflegen. Das Programm netstat verwendet die Informationen in dieser Datenbank zum Erzeugen der Statustabellen.

Beispiel einer /etc/networks-Datei:

BEISPIEL 10–9 /etc/networks-Datei

```
#ident    "@(#)networks    1.4    92/07/14 SMI"    /* SVr4.0 1.1    */
#
# The networks file associates Internet Protocol (IP) network
# numbers with network names. The format of this file is:
#
#     network-name              network-number              nicnames . . .

# The loopback network is used only for intra-machine communication
```

BEISPIEL 10–9 /etc/networks-Datei *(Fortsetzung)*

```
loopback              127

#
# Internet networks
#
arpanet     10       arpa  # Historical
#
# local networks

eng   192.168.9 #engineering
acc   192.168.5 #accounting
prog  192.168.2 #programming
```

protocols-Datenbank

Die protocols-Datenbank enthält die auf Ihrem System installierten TCP/IP-Protokolle sowie deren Protokollnummern. Diese Datenbank wird automatisch vom Oracle Solaris-Installationsprogramm erstellt. Für diese Datenbank ist nur selten ein Benutzereingriff erforderlich.

Die Syntax dieser Datenbank ist in der Manpage protocols(4) beschrieben. Beispiel einer /etc/inet/protocols-Datei:

BEISPIEL 10–10 /etc/inet/protocols-Datei

```
#
# Internet (IP) protocols
#
ip    0   IP    # internet protocol, pseudo protocol number
icmp  1   ICMP  # internet control message protocol
tcp   6   TCP   # transmission control protocol
udp  17   UDP   # user datagram protocol
```

Services-Datenbank

Die Services-Datenbank enthält die Namen der TCP- und UDP-Services und deren bekannte Portnummern. Die Datenbank wird von Programmen verwendet, die Netzwerkservices aufrufen. Die Services-Datenbank wird automatisch vom Oracle Solaris-Installationsprogramm erstellt. Im Allgemeinen ist für diese Datenbank kein Benutzereingriff erforderlich.

Vollständige Informationen zur Syntax finden Sie in der Manpage services(4) Auszug einer typischen /etc/inet/services-Datei:

BEISPIEL 10–11 `/etc/inet/services`-Datei

```
#
# Network services
#
echo       7/udp
echo       7/tcp
echo       7/sctp6
discard    9/udp     sink null
discard    11/tcp
daytime    13/udp
daytime    13/tcp
netstat    15/tcp
ftp-data   20/tcp
ftp        21/tcp
telnet     23/tcp
time       37/tcp    timeserver
time       37/udp    timeserver
name       42/udp    nameserver
whois      43/tcp    nickname
```

Routing-Protokolle in Oracle Solaris

In diesem Abschnitt werden zwei Routing-Protokolle beschrieben, die von Oracle Solaris 10 unterstützt werden): Routing Information Protocol (RIP) und ICMP Router Discovery (RDISC). RIP und RDISC sind TCP/IP-Standardprotokolle. Eine vollständige Liste der in Oracle Solaris 10 verfügbaren Routing-Protokolle finden Sie in Tabelle 5–1 und Tabelle 5–2.

Routing Information Protocol (RIP)

RIP wird von `in.routed` , dem Routing-Daemon implementiert, der beim Booten des Systems automatisch gestartet wird. Wird der `in.routed`-Daemon auf einem Router mit der Option `s` ausgeführt, füllt er die Kernel-Routing-Tabelle mit einer Route zu jedem erreichbaren Netzwerk aus und meldet die „Erreichbarkeit" an alle Netzwerkschnittstellen.

Wenn der `in.routed`-Daemon auf einem Host mit der Option `q` ausgeführt wird, extrahiert er zwar die Routing-Informationen, gibt aber die Erreichbarkeit nicht bekannt. Routing-Informationen auf Hosts können auf zwei Arten extrahiert werden:

- Geben Sie *nicht* das Flag `S` („S" als Großbuchstabe: „Platz sparender Modus" an). `in.routed` erstellt, genauso wie auf einem Router, eine vollständige Routing-Tabelle.
- Geben Sie das Flag `S` an. `in.routed` erstellt eine minimale Kernel-Tabelle, die eine Standardroute zu jedem verfügbaren Router enthält.

ICMP Router Discovery (RDISC)-Protokoll

Hosts verwenden RDISC, um Routing-Informationen von Routern zu beziehen. Wenn Hosts RDISC ausführen, müssen Router noch ein weiteres Protokoll ausführen, z. B. RIP, um Router-Informationen auszutauschen.

RDISC wird vom `in.routed`-Daemon implementiert, der auf Routern und Hosts ausgeführt werden muss. Auf Hosts verwendet der `in.routed`-Daemon RDISC, um die Standardrouten von Routern zu erfassen, die sich selbst über RDISC melden. Auf Routern verwendet der `in.routed`-Daemon RDISC, um Standardrouten zu Hosts in direkt verbundenen Netzwerken bekannt zu geben. Weitere Informationen finden Sie in den Manpages `in.routed`(1M) und `gateways`(4).

Netzwerkklassen

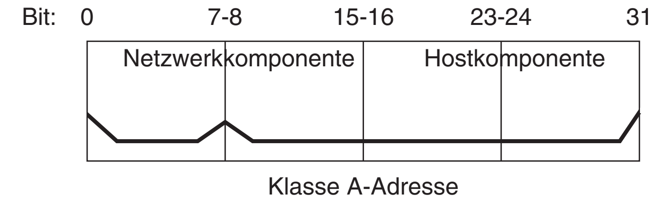
Hinweis – Klassenbasierte Netzwerknummern werden von der IANA nicht mehr vergeben, obwohl verschiedene ältere Netzwerke noch immer klassenbasiert sind.

Dieser Abschnitt enthält ausführliche Informationen zu IPv4-Netzwerkklassen. Jede Klasse verwendet den 32-Bit-IPv4-Adressraum anders und stellt mehr oder weniger Bit als Netzwerkkomponenten der Adresse zur Verfügung. Die Klassen sind Klasse A, Klasse B und Klasse C.

Klasse A-Netzwerknummern

Eine Klasse A-Netzwerknummer verwendet die ersten acht Bit der IPv4-Adresse als „Netzwerkkomponente “. Die verbleibenden 24 Bit enthalten die Hostkomponente der IPv4 Adresse. Dies wird in der folgenden Abbildung verdeutlicht.

ABBILDUNG 10–3 Byte-Zuweisung in einer Klasse A-Adresse

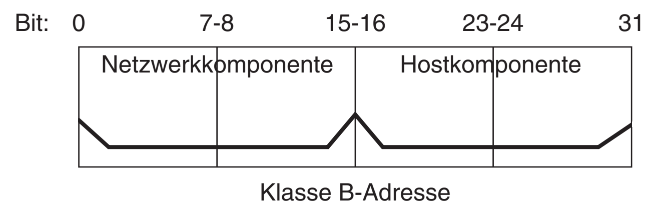


Die Werte, die dem ersten Byte einer Klasse A-Netzwerknummer zugeordnet werden, liegen im Bereich von 0–127. Betrachten Sie die IPv4-Adresse `75.4.10.4`. Der Wert 75 im ersten Byte kennzeichnet, dass sich der Host in einem Klasse A-Netzwerk befindet. Die verbleibenden Byte `4.10.4` geben die Hostadresse an. Nur das erste Byte einer Klasse A-Nummer ist bei der IANA registriert. Die Verwendung der verbleibenden 3 Byte obliegt dem Eigentümer der Netzwerknummer. Es existieren nur 127 Klasse A-Netzwerke. Jede dieser Zahlen kann maximal 16.777.214 Hosts aufnehmen.

Klasse B-Netzwerknummern

Eine Klasse B-Netzwerknummer verwendet 16 Bit für die Netzwerknummer und 16 Bit für die Hostnummern. Das erste Byte einer Klasse B-Netzwerknummer liegt im Bereich 128–191. In der Zahlengruppe `172.16.50.56` sind die ersten 2 Byte, `172.16`, bei der IANA registriert und bilden die Netzwerkadresse. Die letzten 2 Byte, `50.56`, enthalten die Hostadresse. Die Zuweisung obliegt dem Eigentümer der Netzwerknummer. Eine Klasse B-Adresse wird in der folgenden Abbildung dargestellt.

ABBILDUNG 10–4 Byte-Zuweisung in einer Klasse B-Adresse

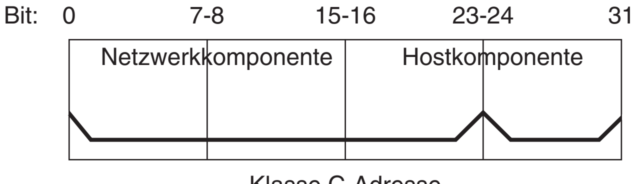


Die Klasse B wird im Allgemeinen Organisationen zugewiesen, deren Netzwerk viele Hosts enthalten.

Klasse C-Netzwerknummern

Eine Klasse C-Netzwerknummer verwendet 24 Bit für die Netzwerknummer und 8 Bit für die Hostnummern. Klasse C-Netzwerknummern eignen sich für Netzwerke mit nur wenigen Hosts (maximal 254). Eine Klasse C-Netzwerknummer belegt die ersten drei Byte einer IPv4-Adresse. Nur die Zuweisung des vierten Byte obliegt den Eigentümern des Netzwerks. Die Byte in einer Klasse C-Adresse sind in der folgenden Abbildung grafisch dargestellt.

ABBILDUNG 10–5 Byte-Zuweisung in einer Klasse C-Adresse



Das erste Byte einer Klasse C-Netzwerknummer liegt im Bereich 192–223. Das zweite und dritte Byte decken jeweils den Bereich 1– 255 ab. Eine typische Klasse C-Adresse ist z. B. `192.168.2.5`. Die ersten 3 Byte, `192.168.2`, bilden die Netzwerknummer. Das letzte Byte in diesem Beispiel, `5`, ist die Hostnummer.

KAPITEL 11

IPv6 im Detail (Referenz)

Dieses Kapitel enthält die folgenden Referenzinformationen zur Implementierung von IPv6 in Oracle Solaris.

- „Weiterführende IPv6-Adressierungsformate" auf Seite 278
- „Format der IPv6-Paket-Header" auf Seite 281
- „Dual-Stack-Protokolle" auf Seite 283
- „Oracle Solaris 10 IPv6-Implementierung" auf Seite 284
- „IPv6 Neighbor Discovery-Protokoll" auf Seite 299
- „IPv6-Routing" auf Seite 306
- „IPv6-Tunnel" auf Seite 308
- „IPv6-Erweiterungen zu den Oracle Solaris-Namen-Services" auf Seite 316
- „NFS und RPC IPv6-Unterstützung" auf Seite 318
- „Unterstützung für IPv6-über-ATM" auf Seite 318

Eine Übersicht der IPv6-Konzepte finden Sie in Kapitel 3, „Einführung in IPv6 (Überblick)". Aufgaben zur Konfiguration eines IPv6-konformen Netzwerks finden Sie in Kapitel 7, „Konfigurieren eines IPv6-Netzwerks (Vorgehen)".

Neuerungen in diesem Kapitel

Unter Solaris 10 7/07 wird die `/etc/inet/ipnodes`-Datei nicht mehr benötigt. Verwenden Sie `/etc/inet/ipnodes` nur für frühere Oracle Solaris 10-Versionen, wie es in den jeweiligen Verfahren beschrieben wird.

Weiterführende IPv6-Adressierungsformate

In Kapitel 3, „Einführung in IPv6 (Überblick)“ wurden die am häufigsten verwendeten IPv6-Adressierungsformate vorgestellt: Unicast-Standortadresse und Link-lokale Adresse. In diesem Abschnitt finden Sie detaillierte Erklärungen der in Kapitel 3, „Einführung in IPv6 (Überblick)“ nicht beschriebenen Adressierungsformate:

- „Von 6to4 abgeleitete Adressen“ auf Seite 278
- „IPv6-Multicast-Adressen im Detail“ auf Seite 280

Von 6to4 abgeleitete Adressen

Wenn Sie beabsichtigen, einen 6to4-Tunnel von einem Router- oder einem Host-Endpunkt zu konfigurieren, müssen Sie das 6to4-Standortpräfix in der `/etc/inet/ndpd.conf`-Datei auf dem System mit dem Endpunkt bekannt geben. Eine Einführung in die Konfiguration von 6to4-Tunneln und zugehörige Aufgaben finden Sie in unter „So konfigurieren Sie einen 6to4-Tunnel“ auf Seite 208.

Die nächste Abbildung zeigt die Komponenten eines 6to4-Standortpräfix.

ABBILDUNG 11–1 Komponenten eines 6to4-Standortpräfix

Format: 6to4-Präfix | IPv4-Adresse
16 bits | 32 bits

Beispiel einer 6to4-Adresse: 2002:8192:5666::/48

Beispielformat: 2002 : 8192.5666 :: /48
Präfix | IPv4-Adresse | Präfixlänge (48 Bit)

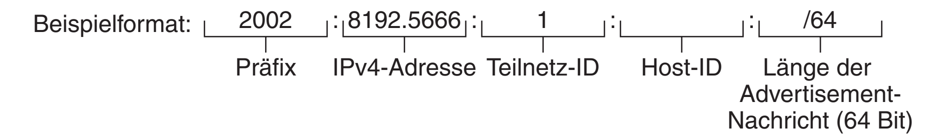
Die nächste Abbildung zeigt die Komponenten eines Teilnetzpräfix für einen 6to4-Standort, die Sie in die `ndpd.conf`-Datei aufnehmen würden.

ABBILDUNG 11–2 Komponenten eines 6to4-Teilnetzpräfix

Format: 6to4-Präfix | IPv4-Adresse | Subnet: Host

16 Bit | 32 Bit | 16 Bit

Beispiel einer 6to4-Adresse: 2002:8192.5666:1: :/64



In dieser Tabelle werden die Komponenten eines 6to4-Teilnetzpräfix erklärt, sowie deren Längen und Definitionen.

Komponente	Länge	Definition
Präfix	16 Bit	6to4-Präfix-Label 2002 (0x2002).
IPv4-Adresse	32 Bit	Einmalige IPv4-Adresse, die bereits auf der 6to4-Schnittstelle konfiguriert ist. Zur Bekanntgabe geben Sie die hexadezimale Darstellung der IPv4-Adresse anstelle der getrennten dezimalen Notation an.
Teilnetz-ID	16 Bit	Teilnetz-ID; dieser Wert muss einmalig für den Link an Ihrem 6to4-Standort sein.

Von 6to4 abgeleitete Adressierung auf einem Host

Wenn ein IPv6-Host das von 6to4 abgeleitete Präfix über eine Router-Advertisement-Nachricht empfängt, konfiguriert der Host automatisch eine von 6to4 abgeleitete Adresse auf der Schnittstelle. Die Adresse hat das folgende Format:

prefix:IPv4-address:subnet-ID:interface-ID`/64`

Die Ausgabe des Befehls `ifconfig -a` auf einem Host mit einer 6to4-Schnittstelle ähnelt dem Folgenden:

```
qfe1:3: flags=2180841<UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6>
 mtu 1500 index 7
        inet6 2002:8192:56bb:9258:a00:20ff:fea9:4521/64
```

In dieser Ausgabe folgt die von 6to4 abgeleitete Adresse `inet6`.

In der folgenden Tabelle werden die Komponenten der von 6to4 abgeleiteten Adresse erklärt, sowie die Längen der Komponenten und die von den Komponenten bereitgestellten Informationen.

Adresskomponente	Länge	Definition
prefix	16 Bit	`2002`, das 6to4-Präfix
IPv4-Adresse	32 Bit	`8192:56bb`, die IPv4-Adresse in hexadezimaler Notation für die 6to4-Pseudoschnittstelle, die auf dem 6to4-Router konfiguriert ist
Teilnetz-ID	16 Bit	`9258`, die Adresse des Teilnetzes, in dem dieser Host Mitglied ist
Schnittstellen-ID	64 Bit	`a00:20ff:fea9:4521`, die Schnittstellen-ID der Host-Schnittstelle, die für 6to4 konfiguriert ist

IPv6-Multicast-Adressen im Detail

Mit einer IPv6-Multicast-Adresse können identische Informationen oder Services an eine definierte Schnittstellengruppe, die so genannte *Multicast-Gruppe*, verteilt werden. In der Regel befinden sich die Schnittstellen einer Multicast-Gruppe auf verschiedenen Knoten. Eine Schnittstelle kann mehreren Multicast-Gruppen angehören. Pakete, die an die Multicast-Adresse gesendet werden, werden an alle Mitglieder der Multicast-Gruppe geleitet. Eine Verwendungsmöglichkeit von Multicast-Adressen ist das Broadcasten von Informationen, ähnlich den Funktionen der IPv4-Broadcast-Adresse.

In der folgenden Tabelle wird das Format der Multicast-Adresse vorgestellt.

TABELLE 11–1 Format der IPv6-Multicast-Adresse

8 Bit	4 Bit	4 Bit	8 Bit	8 Bit	64 Bit	32 Bit
`11111111`	*FLGS*	`SCOP`	*Reserviert*	*Plen*	*Netzwerkpräfix*	*Gruppen-ID*

Im Folgenden werden die Inhalte jedes Feldes beschrieben.

- `11111111` – Kennzeichnet die Adresse als Multicast.
- *FLGS* – Satz der vier Flags 0,0,P,T. Die ersten zwei Flags müssen 0 sein. Das Feld P nimmt einen der beiden folgenden Werte an:
  - 0 = Multicast-Adresse, die nicht auf dem Netzwerkpräfix basierend zugewiesen wurde
  - 1 = Multicast-Adresse, die basierend auf dem Netzwerkpräfix zugewiesen wurde

  Wenn P auf 1 gesetzt ist, muss T ebenfalls auf 1 gesetzt sein.
- *Reserviert* - Reserviert für den Wert null.
- *Plen* - Anzahl der Bit im Standortpräfix, die das Teilnetz für eine Multicast-Adresse identifizieren, die basierend auf einem Standortpräfix zugewiesen wurde.
- *Gruppen-ID* - Bezeichner für die Multicast-Gruppe, entweder permanent oder dynamisch.

Ausführliche Informationen zum Multicast-Format finden Sie in RFC 3306, „Unicast-Prefix-based IPv6 Multicast Addresses (`ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt`).

Einige IPv6-Multicast-Adressen sind permanent von der Internet Assigned Numbers Authority (IANA) zugewiesen. Beispiele dieser Adressen sind All Nodes Multicast Addresses und All Routers Multicast Addresses, die für alle IPv6-Hosts und -Routern erforderlich sind. IPv6-Multicast-Adressen können auch dynamisch zugewiesen werden. Weitere Informationen zur ordnungsgemäßen Verwendung von Multicast-Adressen und -Gruppen finden Sie in RFC 3307, „Allocation Guidelines for IPv6 Multicast Addresses.

Format der IPv6-Paket-Header

Das IPv6-Protokoll definiert eine Reihe von Headern, einschließlich dem einfachen IPv6-Header und dem IPv6-Extension-Header. In der folgenden Abbildung werden die Felder in einem IPv6-Header und die Reihenfolge dieser Felder gezeigt.

ABBILDUNG 11–3 Format eines einfachen IPv6-Header

<table>
<tr><td>Version</td><td>Verkehrsklasse</td><td colspan="2">Flow-Label</td></tr>
<tr><td colspan="2">Nutzlastlänge</td><td>Nächster Header</td><td>Hop-Grenzwert</td></tr>
<tr><td colspan="4">Ursprungsadresse</td></tr>
<tr><td colspan="4">Zieladresse</td></tr>
</table>

Die folgende Liste beschreibt die Funktionen jedes Header-Feldes.

- **Version** – 4-Bit-Versionsnummer des Internet-Protokolls = 6.
- **Verkehrsklasse** – Feld in der Länge 8 Bit für die Verkehrsklasse.
- **Fluss-Label** – Feld in der Länge 20 Bit.
- **Nutzlastlänge** – Vorzeichenloser, ganzzahliger Wert in der Länge 16 Bit; der Rest des Pakets, der dem IPv6-Header folgt, in Oktetten.

- **Nächster Header** – Selektor in der Länge 8 Bit. Gibt den Headertyp an, der dem IPv6-Header unmittelbar folgt. Verwendet die gleichen Werte wie das IPv4-Protokollfeld
- **Hop-Grenzwert** – Vorzeichenloser, ganzzahliger Wert in der Länge 8 Bit. Wird von jedem Knoten, der das Paket weiterleitet, um 1 verringert. Das Paket wird abgeworfen, wenn die Hop-Grenzwert auf null verringert wurde.
- **Quelladresse** – 128 Bit. Die Adresse des ursprünglichen Senders des Pakets.
- **Zieladresse** – 128 Bit. Die Adresse des geplanten Empfängers des Pakets. Der geplante Empfänger muss nicht unbedingt der Empfänger sein, wenn ein optionaler Routing-Header vorhanden ist.

IPv6-Extension-Header

IPv6-Optionen werden in separaten Extension-Headern platziert, die sich zwischen dem IPv6-Header und dem Transportschicht-Header in einem Paket befinden. Die meisten IPv6-Extension-Header werden von den Routern im Zustellungspfad eines Pakets weder geprüft noch verarbeitet, bis das Paket an seinem endgültigen Ziel eintrifft. Diese Funktion stellt für Pakete, die Optionen enthalten, eine wesentliche Verbesserung der Router-Performance dar. Bei IPv4 wird durch die Angabe einer Option erforderlich, dass der Router alle Optionen untersucht.

Im Gegensatz zu IPv4-Optionen können IPv6-Extension-Header eine beliebige Länge annehmen, und die Anzahl an Optionen, die ein Paket enthalten kann, ist nicht auf 40 Byte beschränkt. Diese Funktion (neben der Art und Weise, wie IPv6-Optionen verarbeitet werden), ermöglicht es, dass IPv6-Optionen für Funktionen verwendet werden, deren Umsetzung unter IPv4 nicht möglich wäre.

Um die Performance bei der Verarbeitung von nachfolgenden Option-Headern und dem darauf folgenden Transportprotokoll zu verbessern, sind IPv6-Optionen immer ein ganzzahliges Vielfaches mit einer Länge von 8 Oktetten. Das ganzzahlige Vielfache von 8 Oktetten behält die Gruppierung der nachfolgenden Header bei.

Folgende IPv6-Extension-Header sind derzeit definiert:

- **Routing** – Erweitertes Routing, z. B. lose IPv4-Quellroute
- **Fragmentierung** – Fragmentierung und Neuassemblierung
- **Authentifizierung** – Integrität und Authentifizierung und Sicherheit
- **Einkapselung der Sicherheitsnutzlast** – Vertraulichkeit
- **Hop-by-Hop Optionen** – Spezielle Optionen, die eine Hop-by-Hop-Verarbeitung erfordern
- **Zieloptionen** – Optionale Informationen, die vom Zielknoten untersucht werden

Dual-Stack-Protokolle

Der Begriff *Dual-Stack* bezieht sich in der Regel auf eine vollständige Duplikation aller Ebenen im Protokollstapel, von der Anwendungs- bis zur Netzwerkschicht. Ein Beispiel einer vollständigen Duplikation ist ein System, das sowohl OSI- als auch TCP/IP-Protokolle ausführt.

Oracle Solaris ist *Dual-Stack*-konform. Dies bedeutet, dass Oracle Solaris sowohl das IPv4- als auch das IPv6-Protokoll implementieren kann. Bei der Installation des Betriebssystems können Sie wählen, ob die IPv6-Protokolle auf der IP-Schicht oder ob nur die standardmäßigen IPv4-Protokolle aktiviert werden. Der übrige TCP/IP-Stapel ist identisch. Entsprechend können die gleichen Transportprotokolle, TCP, UDP und SCTP, sowohl über IPv4 als auch über IPv6 ausgeführt werden. Außerdem können die gleichen Anwendungen sowohl über IPv4 als auch über IPv6 ausgeführt werden. Abbildung 11–4 zeigt, wie die IPv4- und IPv6-Protokolle über die verschiedenen Ebenen der Internet-Protokollfamilie als Dual-Stack arbeiten.

ABBILDUNG 11–4 Architektur eines Dual-Stack-Protokolls

Bei diesem Dual-Stack-Szenario werden Gruppen von Hosts und Routern neben der Unterstützung von IPv4 zur Unterstützung auf IPv6 aufgerüstet. Der Dual-Stack-Ansatz stellt sicher, dass die aufgerüsteten Knoten immer über IPv4 mit nur-IPv4-Knoten zusammenarbeiten können.

Oracle Solaris 10 IPv6-Implementierung

In diesem Abschnitt werden die Dateien, Befehle und Daemons beschrieben, mit denen IPv6 in Oracle Solaris implementiert wird.

IPv6-Konfigurationsdateien

In diesem Abschnitt werden die Konfigurationsdateien beschrieben, die Teil einer IPv6-Implementierung sind:

- „ndpd.conf-Konfigurationsdatei" auf Seite 284
- „IPv6-Schnittstellenkonfigurationsdatei" auf Seite 288
- „/etc/inet/ipaddrsel.conf-Konfigurationsdatei" auf Seite 289

ndpd.conf-Konfigurationsdatei

Die /etc/inet/ndpd.conf-Datei dient zur Konfiguration von Optionen, die vom Neighbor Discovery-Daemon in.ndpd verwendet werden. Bei einem Router verwenden Sie ndpd.conf hauptsächlich zur Konfiguration des Standortpräfix, das auf dem Link bekannt gegeben wird. Bei einem Host verwenden Sie ndpd.conf zum Deaktivieren der automatischen Adresskonfiguration oder zur Konfiguration von temporären Adressen.

Die folgende Tabelle zeigt die Schlüsselwörter, die in der ndpd.conf-Datei verwendet werden.

TABELLE 11–2 /etc/inet/ndpd.conf -Schlüsselwörter

Variable	Beschreibung
ifdefault	Gibt das Router-Verhalten für alle Schnittstellen an. Zum Einrichten der Router-Parameter und der zugehörigen Werte verwenden Sie die folgende Syntax: ifdefault [*Variablenwert*]
prefixdefault	Gibt das Standardverhalten für Präfix-Advertisement-Nachrichten an. Zum Einrichten der Router-Parameter und der zugehörigen Werte verwenden Sie die folgende Syntax: prefixdefault [*Variablenwert*]
if	Richtet die Parameter für eine Schnittstelle ein. Verwenden Sie die folgende Syntax: if *Schnittstelle* [*Variablenwert*]
prefix	Gibt Präfix-Informationen für eine Schnittstelle bekannt. Verwenden Sie die folgende Syntax: prefix *Präfix/Länge Schnittstelle* [*Variablenwert*]

In der `ndpd.conf`-Datei können Sie die Schlüsselwörter in der folgenden Tabelle mit bestimmten Router-Konfigurationsvariablen verwenden. Diese Variables werden ausführlich in RFC 2461, Neighbor Discovery for IP Version 6 (IPv6) (`http://www.ietf.org/rfc/rfc2461.txt?number=2461`) definiert.

Die nächste Tabelle zeigt die Variablen zur Konfiguration einer Schnittstelle und definiert diese kurz.

TABELLE 11–3 `/etc/inet/ndpd.conf`-Variablen zur Schnittstellenkonfiguration

Variable	Standard	Definition
`AdvRetransTimer`	0	Legt den Wert im Feld „Retrans Timer" der Advertisement-Nachrichten vom Router fest.
`AdvCurHopLimit`	Aktueller Durchmesser des Netzwerks	Gibt den Wert an, der in den aktuellen Hop-Grenzwert in den Advertisement-Nachrichten vom Router eingefügt wird.
`AdvDefaultLifetime`	3 + `MaxRtrAdvInterval`	Gibt die standardmäßige Lebensdauer von Router Advertisement-Nachrichten an.
`AdvLinkMTU`	0	Gibt den Wert für eine Maximum Transmission Unit (MTU) an, die vom Router gesendet wird. Null kennzeichnet, dass der Router keine MTU-Optionen angibt.
`AdvManaged Flag`	False	Gibt den Wert an, der in das Manage Address Configuration-Flag in der Router Advertisement-Nachricht eingefügt wird.
`AdvOtherConfigFlag`	False	Gibt den Wert an, der in das Other Stateful Configuration-Flag in der Router Advertisement-Nachricht eingefügt wird.
`AdvReachableTime`	0	Legt den Wert im Feld „Reachable Time" in den Advertisement-Nachrichten vom Router fest.
`AdvSendAdvertisements`	False	Gibt an, ob der Knoten Advertisement-Nachrichten senden und auf Router Solicitation-Nachrichten reagieren soll. Sie müssen diese Variable in der `ndpd.conf`-Datei explizit auf „TRUE" setzen, um die Funktionen der Router Advertisement-Nachrichten zu aktivieren. Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie einen IPv6-konformen Router" auf Seite 192.
`DupAddrDetect` `Transmits`	1	Definiert die Anzahl an aufeinander folgenden Neighbor Solicitation-Nachrichten, die das Neighbor Discovery-Protokoll senden soll, wenn die Adresse des lokalen Knotens doppelt erfasst wurde.
`MaxRtrAdvInterval`	600 Sekunden	Gibt die maximale Dauer zwischen dem Senden von nicht angeforderten Multicast Advertisement-Nachrichten an.
`MinRtrAdvInterval`	200 Sekunden	Gibt die Mindestdauer zwischen dem Senden von nicht angeforderten Multicast Advertisement-Nachrichten an.

TABELLE 11–3 `/etc/inet/ndpd.conf`-Variablen zur Schnittstellenkonfiguration *(Fortsetzung)*

Variable	Standard	Definition
`StatelessAddrConf`	True	Legt fest, ob der Knoten seine IPv6-Adresse über die statusfreie automatische Adresskonfiguration konfiguriert. Wenn „False“ in der Datei `ndpd.conf` angegeben ist, muss die Adresse manuell konfiguriert werden. Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie ein benutzerdefiniertes IPv6-Token“ auf Seite 200.
`TmpAddrsEnabled`	False	Gibt an, ob eine temporäre Adresse für alle Schnittstellen oder für eine bestimmte Schnittstelle eines Knotens konfiguriert werden soll. Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie eine temporäre Adresse“ auf Seite 197.
`TmpMaxDesyncFactor`	600 Sekunden	Liefert einen Zufallswert an, der für die bevorzugte Lebensdauer `TmpPreferredLifetime` von der Variablen subtrahiert wird, wenn `in.ndpd` startet. Der Zweck der Variablen `TmpMaxDesyncFactor` besteht darin, zu verhindern, dass alle Systeme in Ihren Netzwerken ihre temporären Adressen gleichzeitig neu generieren. `TmpMaxDesyncFactor` ermöglicht Ihnen das Ändern des oberen Grenzwerts für diesen Zufallswert.
`TmpPreferredLifetime`	False	Legt die bevorzugte Lebensdauer einer temporären Adresse fest. Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie eine temporäre Adresse“ auf Seite 197.
`TmpRegenAdvance`	False	Legt die Vorlaufzeit vor dem Ablauf einer Adresse für eine temporäre Adresse fest. Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie eine temporäre Adresse“ auf Seite 197.
`TmpValidLifetime`	False	Legt die gültige Lebensdauer einer temporären Adresse fest. Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie eine temporäre Adresse“ auf Seite 197.

Die nächste Tabelle zeigt die Variablen zur Konfiguration von IPv6-Präfixen.

TABELLE 11–4 `/etc/inet/ndpd.conf` -Variablen zur Präfixkonfiguration

Variable	Standard	Definition
`AdvAutonomousFlag`	True	Gibt den Wert an, der in das Feld „Autonomes Flag“ der Option „Präfixinformationen“ eingefügt wird.
`AdvOnLinkFlag`	True	Gibt den Wert an, der in das On-link Flag („L-bit“) in der Option „Präfixinformationen“ eingefügt wird.
`AdvPreferredExpiration`	Nicht gesetzt	Gibt das bevorzugte Ablaufdatum des Präfix an.
`AdvPreferredLifetime`	604800 Sekunden	Gibt den Wert an, der für die bevorzugte Lebensdauer in der Option „Präfixinformationen“ eingefügt wird.

TABELLE 11–4 `/etc/inet/ndpd.conf` -Variablen zur Präfixkonfiguration *(Fortsetzung)*

Variable	Standard	Definition
`AdvValidExpiration`	Nicht gesetzt	Gibt das gültige Ablaufdatum des Präfix an.
`AdvValidLifetime`	2592000 Sekunden	Gibt die gültige Lebensdauer des zu konfigurierenden Präfix an.

BEISPIEL 11–1 `/etc/inet/ndpd.conf`-Datei

Das folgende Beispiel zeigt, wie die Schlüsselwörter und Konfigurationsvariablen in der Datei `ndpd.conf` verwendet werden. Löschen Sie die Kommentarzeichen (#), um die Variable zu aktivieren.

```
# ifdefault      [variable-value ]*
# prefixdefault [variable-value ]*
# if ifname    [variable-value ]*
# prefix prefix/length ifname
#
#  Per interface configuration variables
#
#DupAddrDetectTransmits
#AdvSendAdvertisements
#MaxRtrAdvInterval
#MinRtrAdvInterval
#AdvManagedFlag
#AdvOtherConfigFlag
#AdvLinkMTU
#AdvReachableTime
#AdvRetransTimer
#AdvCurHopLimit
#AdvDefaultLifetime
#
# Per Prefix:  AdvPrefixList configuration variables
#
#
#AdvValidLifetime
#AdvOnLinkFlag
#AdvPreferredLifetime
#AdvAutonomousFlag
#AdvValidExpiration
#AdvPreferredExpiration

ifdefault AdvReachableTime 30000 AdvRetransTimer 2000
prefixdefault AdvValidLifetime 240m AdvPreferredLifetime 120m

if qe0 AdvSendAdvertisements 1
prefix 2:0:0:56::/64 qe0
prefix fec0:0:0:56::/64 qe0

if qe1 AdvSendAdvertisements 1
prefix 2:0:0:55::/64 qe1
prefix fec0:0:0:56::/64 qe1

if hme1 AdvSendAdvertisements 1
prefix  2002:8192:56bb:1::/64 qfe0

if hme1 AdvSendAdvertisements 1
```

BEISPIEL 11–1 `/etc/inet/ndpd.conf`-Datei *(Fortsetzung)*

```
prefix  2002:8192:56bb:2::/64 hme1
```

IPv6-Schnittstellenkonfigurationsdatei

IPv6 verwendet die `/etc/hostname6.`*Schnittstelle*-Datei beim Booten, um die logischen IPv6-Schnittstellen automatisch zu definieren. Wenn Sie während der Oracle Solaris-Installation die Option ?IPv6-konform“ ausgewählt haben, erstellt das Installationsprogramm neben der `/etc/hostname.`-*Schnittstellendatei*eine `/etc/hostname6.`-*Schnittstellendatei* für die primäre Netzwerkschnittstelle.

Erfasst das Installationsprogramm weitere physikalische Schnittstellen, werden Sie aufgefordert, auch diese Schnittstellen zu konfigurieren. Für jede zusätzliche Schnittstelle, die Sie auswählen, erstellt das Installationsprogramm Konfigurationsdateien für physikalische IPv4-Schnittstellen und für logische IPv6-Schnittstellen.

Wie IPv4-Schnittstellen können Sie auch IPv6-Schnittstellen nach der Oracle Solaris-Installation manuell konfigurieren. In diesem Fall liegen Sie `/etc/hostname6.`*Schnittstelle*-Dateien für die neuen Schnittstellen an. Anweisungen zur manuellen Konfiguration von Schnittstellen finden Sie unter „Verwalten der Schnittstellen in Solaris 10 3/05“ auf Seite 147 oderKapitel 6, „Verwalten von Netzwerkschnittstellen (Aufgaben)“.

Eine Konfigurationsdatei für eine Netzwerkschnittstelle muss die folgende Syntax aufweisen:

`hostname.`*interface*
`hostname6.`*interface*

Die Variable *Schnittstelle* hat die folgende Syntax:

dev`[.`*module*`[.`*module* `...]]`*PPA*

Gerät Gibt ein Netzwerkschnittstellengerät an. Bei diesem Gerät kann es sich um eine physikalische Schnittstelle, z. B. `eri` oder `qfe`, oder um eine logische Schnittstelle, zum Beispiel einen Tunnel handeln. Weitere Informationen hierzu finden Sie unter „IPv6-Schnittstellenkonfigurationsdatei“ auf Seite 288.

Modul Führt mindestens ein `STREAMS`-Modul auf, das dem Gerät beim Plumben (Aktivieren) zugewiesen wird.

PPA Gibt den physikalischen Anschlusspunkt an.

Die Syntax [.[.]] ist ebenfalls zulässig.

BEISPIEL 11–2 IPv6-Schnittstellenkonfigurationsdateien

Im Folgenden sind Beispiele für gültige Namen einer IPv6-Konfigurationsdatei aufgeführt:

BEISPIEL 11–2 IPv6-Schnittstellenkonfigurationsdateien *(Fortsetzung)*

```
hostname6.qfe0
hostname.ip.tun0
hostname.ip6.tun0
hostname6.ip6to4tun0
hostname6.ip.tun0
hostname6.ip6.tun0
```

/etc/inet/ipaddrsel.conf-**Konfigurationsdatei**

Die Datei /etc/inet/ipaddrsel.conf enthält die Richtliniendatei für eine standardmäßige IPv6-Adressauswahl. Wenn Sie Oracle Solaris so installieren, dass IPv6 aktiviert ist, hat diese Datei den in Tabelle 11–5 gezeigten Inhalt.

Der Inhalt von /etc/inet/ipaddrsel.conf kann geändert werden. In den meisten Fällen wird jedoch von der Bearbeitung dieser Datei abgeraten. Falls eine Bearbeitung erforderlich wird, verwenden Sie das unter „So verwalten Sie die Richtlinientabelle zur IPv6-Adressauswahl“ auf Seite 243 beschriebene Verfahren. Weitere Informationen zur ippaddrsel.conf-Datei finden Sie unter „Gründe zur Bearbeitung der Richtlinientabelle für die IPv6-Adressauswahl“ auf Seite 290 und in der Manpage ipaddrsel.conf(4).

IPv6-bezogene Befehle

In diesem Abschnitt werden die Befehle beschrieben, die mit der IPv6-Implementierung zu Oracle Solaris hinzugefügt werden. Hier werden auch die Modifikationen an vorhandenen Befehlen beschrieben, um IPv6 zu unterstützen.

ipaddrsel-**Befehl**

Mit dem Befehl ipaddrsel können Sie die Richtlinientabelle für die IPv6-Standard-Adressauswahl bearbeiten.

Der Oracle Solaris-Kernel verwendet die Richtlinientabelle für die IPv6-Standard-Adressauswahl, um die Zieladressen in eine Reihenfolge zu bringen und die Quelladresse eines IPv6-Paket-Headers auszuwählen. Die Richtlinientabelle ist in der /etc/inet/ipaddrsel.conf-Datei enthalten.

Die folgenden Tabelle enthält die Standard-Adressformate und deren Prioritäten für die Richtlinientabelle. Ausführliche technische Informationen zur IPv6-Adressenauswahl finden Sie in der Manpage inet6(7P).

TABELLE 11–5 Richtlinientabelle für die IPv6-Adressauswahl

Präfix	Prioritätsstufe	Definition
`::1/128`	50	Loopback
`::/0`	40	Standard
`2002::/16`	30	6to4
`::/96`	20	IPv4-kompatibel
`::ffff:0:0/96`	10	IPv4

In dieser Tabelle haben die IPv6-Präfixe (`::1/128` und `::/0`) Vorrang vor den 6to4-Adressen (`2002::/16`) und den IPv4-Adressen (`::/96` und `::ffff:0:0/96`). Aus diesem Grund wählt der Kernel standardmäßig die globale IPv6-Adresse der Schnittstelle für Pakete, die für ein anderes IPv6-Ziel bestimmt sind. Die IPv4-Adresse der Schnittstelle hat eine geringere Priorität, insbesondere für Pakete, die an einen IPv6-Ziel gerichtet sind. Bei der ausgewählten IPv6-Quelladresse verwendet der Kernel darüber hinaus das IPv6-Format für die Zieladresse.

Gründe zur Bearbeitung der Richtlinientabelle für die IPv6-Adressauswahl

In den meisten Fällen müssen Sie die Richtlinientabelle für die IPv6-Standard-Adressauswahl nicht ändern. Wenn Sie die Richtlinientabelle bearbeiten müssen, verwenden Sie den Befehl `ipaddrsel`.

In den folgenden Fällen können Sie die Richtliniendatei ändern:

- Wenn das System über eine Schnittstelle verfügt, die für ein 6to4-Tunnel verwendet wird, können Sie den 6to4-Adressen eine höhere Priorität zuweisen.
- Wenn Sie möchten, dass eine bestimmte Quelladresse nur bei einem Datenaustausch mit einer bestimmten Zieladresse verwendet wird, können Sie diese Adressen zur Richtliniendatei hinzufügen. Dann priorisieren Sie diese Adressen mit dem Befehl `ifconfig`.
- Wenn Sie möchten, dass IPv4-Adressen eine höhere Prioritätsstufe als IPv6-Adressen einnehmen, können Sie die Priorität `::ffff:0:0/96` zu einem höheren Wert ändern.
- Möchten Sie veralteten Adressen eine höhere Priorität zuweisen, fügen Sie die veraltete Adresse der Richtliniendatei hinzu. Beispielsweise sind Standort-lokale Adressen in IPv6 jetzt veraltet. Diese Adressen haben das Präfix `fec0::/10`. Sie können die Richtlinientabelle jedoch so ändern, dass Standort-lokale Adressen eine höhere Priorität erhalten.

Weitere Informationen zum Befehl `ipaddrsel` finden Sie in der Manpage `ipaddrsel`(1M).

`6to4relay`-Befehl

6to4-Tunneling ermöglicht die Kommunikation zwischen isolierten 6to4-Standorten. Um jedoch Pakete an einen nativen, nicht-6to4 IPv6-Standort zu übertragen, muss der 6to4-Router einen Tunnel zu einem 6to4-Relay-Router einrichten. Der *6to4-Relay-Router* leitet die 6to4-Pakete an das IPv6-Netzwerk und schließlich an den nativen IPv6-Standort. Wenn Ihr 6to4-konformer Standort Daten mit einem nativen IPv6-Standort austauschen muss, können Sie den entsprechenden Tunnel mit dem Befehl `6to4relay` einrichten.

Da die Verwendung von Relais-Routern nicht sicher ist, wird das Tunneling zu einem Relay-Router in Oracle Solaris standardmäßig deaktiviert. Berücksichtigen Sie diese Aspekte beim Erstellen eines Tunnels zu einem 6to4-Relay-Router, bevor Sie dieses Szenario umsetzen. Ausführliche Informationen zu 6to4-Relay-Routern finden Sie unter „Sicherheitsbetrachtungen bei Tunneln zu einem 6to4-Relay-Router“ auf Seite 314. Wenn Sie sich entschließen, die Unterstützung für 6to4-Relay-Router zu implementieren, finden Sie die zugehörigen Verfahren unter „So konfigurieren Sie einen 6to4-Tunnel“ auf Seite 208.

Syntax von `6to4relay`

Der Befehl `6to4relay` weist die folgende Syntax auf:

```
6to4relay -e [-a IPv4-address] -d -h
```

`-e` — Unterstützt Tunnel zwischen dem 6to4-Router und einem Anycast 6to4-Relay-Router. Die Endpunktadresse des Tunnels wird dann auf `192.88.99.1` gesetzt, die Standardadresse für die Anycast-Gruppe der 6to4-Relay-Router.

`-a` *IPv4-Adresse* — Unterstützt Tunnel zwischen dem 6to4-Router und einem 6to4-Relay-Router mit der angegebenen *IPv4-Adresse*.

`-d` — Deaktiviert die Unterstützung für das Tunneling zu einem 6to4-Relay-Router, die Standardeinstellung für Oracle Solaris.

`-h` — Zeigt die Hilfe für `6to4relay` an.

Weitere Informationen finden Sie in der Manpage `6to4relay`(1M).

BEISPIEL 11–3 Standardmäßige Statusanzeige der Unterstützung für 6to4-Relay-Router

Der Befehl `6to4relay` ohne Argumente zeigt den aktuellen Status der Unterstützung für 6to4-Relay-Router an. Das folgende Beispiel zeigt die Standardeinstellung für die Oracle Solaris-Implementierung von IPv6 an.

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is disabled
```

BEISPIEL 11–4 Statusanzeige bei aktivierter Unterstützung für 6to4-Relay-Router

Wenn die Relay-Router-Unterstützung aktiviert ist, liefert der Befehl `6to4relay` die folgende Ausgabe:

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is enabled
IPv4 destination address of Relay Router=192.88.99.1
```

BEISPIEL 11–5 Statusanzeige bei angegebenem 6to4-Relay-Router

Wenn Sie die Option `-a` und eine IPv4-Adresse mit dem Befehl `6to4relay` angeben, wird die mit `-a` angegebene IPv4-Adresse anstelle von `192.88.99.1` angezeigt.

`6to4relay` meldet die erfolgreiche Ausführung der Optionen `-d`, `-e` und `-a` *IPv4-Adresse* nicht. Jedoch zeigt `6to4relay` bei der Ausführung dieser Optionen eventuell generierte Fehlermeldungen an.

`ifconfig`-Befehlserweiterungen zur Unterstützung von IPv6

Mit dem Befehl `ifconfig` können Sie IPv6-Schnittstellen aktivieren und das Tunneling-Modul plumben. `ifconfig` verwendet einen erweiterten Satz ioctls, um sowohl IPv4- als auch IPv6-Netzwerkschnittstellen zu konfigurieren. Im Folgenden werden die `ifconfig`-Optionen für die Unterstützung von IPv6-Vorgängen aufgeführt. Unter „Überwachen der Schnittstellenkonfiguration mit dem Befehl `ifconfig`“ auf Seite 221 finden Sie die IPv4- und IPv6-Aufgaben, die `ifconfig` einbeziehen.

`index`	Richtet den Schnittstellenindex ein.
`tsrc/tdst`	Richtet die Tunnelquelle oder das -ziel ein.
`addif`	Erstellt die nächste verfügbare logische Schnittstelle.
`removeif`	Löscht die logische Schnittstelle mit der angegebenen IP-Adresse.
`destination`	Richtet eine Point-to-Point-Zieladresse für eine Schnittstelle ein.
`set`	Richtet eine Adresse, Netzmaske oder beides für eine Schnittstelle ein.
`subnet`	Richtet die Teilnetzadresse einer Schnittstelle ein.
`xmit/-xmit`	Aktiviert oder deaktiviert die Paketübertragung auf einer Schnittstelle.

Kapitel 7, „Konfigurieren eines IPv6-Netzwerks (Vorgehen)“ enthält Verfahren zur IPv6-Konfiguration.

BEISPIEL 11–6 Hinzufügen einer logischen IPv6-Schnittstelle mit der Option `-addif` des Befehls `ifconfig`

Die folgende Syntax des Befehls `ifconfig` erstellt die logische Schnittstelle `hme0:3`:

BEISPIEL 11–6 Hinzufügen einer logischen IPv6-Schnittstelle mit der Option `-addif` des Befehls `ifconfig` *(Fortsetzung)*

```
# ifconfig hme0 inet6 addif up
Created new logical interface hme0:3
```

Diese Syntax des Befehls `ifconfig` überprüft, ob die neue Schnittstelle korrekt erstellt wurde:

```
# ifconfig hme0:3 inet6
hme0:3: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        inet6  inet6 fe80::203:baff:fe11:b321/10
```

BEISPIEL 11–7 Entfernen einer logischen IPv6-Schnittstelle mit der Option `-removeif` des Befehls `ifconfig`

Die folgende Syntax des Befehls `ifconfig` löscht die logische Schnittstelle `hme0:3`.

```
# ifconfig hme0:3 inet6 down

# ifconfig hme0 inet6 removeif 1234::5678
```

BEISPIEL 11–8 Verwenden des Befehls `ifconfig` zur Konfiguration einer IPv6-Tunnelquelle

```
# ifconfig ip.tun0 inet6 plumb index 13
```

Öffnet einen Tunnel, der dem Namen der physikalischen Schnittstelle zugeordnet wird.

```
# ifconfig ip.tun0 inet6
ip.tun0: flags=2200850<POINTOPOINT,RUNNING,MULTICAST,NONUD,
#IPv6> mtu 1480 index 13
        inet tunnel src 0.0.0.0
        inet6 fe80::/10 --> ::
```

Konfiguriert die Datenströme, die für TCP/IP erforderlich sind, um das Tunnelgerät zu verwenden und den Gerätestatus zu melden.

```
# ifconfig ip.tun0 inet6 tsrc 120.46.86.158 tdst 120.46.86.122
```

Konfiguriert die Quell- und Zieladresse des Tunnels.

```
# ifconfig ip.tun0 inet6
ip.tun0: flags=2200850<POINTOPOINT,RUNNING,MULTICAST,NONUD,
IPv6> mtu 1480 index 13
        inet tunnel src 120.46.86.158  tunnel dst 120.46.86.122
        inet6 fe80::8192:569e/10 --> fe80::8192:567a
```

Meldet dem neuen Gerätestatus nach der Konfiguration.

BEISPIEL 11–9 Konfiguration eines 6to4-Tunnels mithilfe des Befehls `ifconfig` (ausführlich)

Dieses Beispiel für die Konfiguration einer 6to4-Pseudoschnittstelle verwendet die Teilnetz-ID 1 und gibt die Host-ID in hexadezimaler Form an:

BEISPIEL 11–9 Konfiguration eines 6to4-Tunnels mithilfe des Befehls `ifconfig` (ausführlich) *(Fortsetzung)*

```
# ifconfig ip.6to4tun0 inet6 plumb
# ifconfig ip.6to4tun0 inet tsrc 129.146.86.187 \
2002:8192:56bb:1::8192:56bb/64 up

# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NONUD,IPv6>mtu 1480 index 11
        inet tunnel src 129.146.86.187
        tunnel hop limit 60
        inet6 2002:8192:56bb:1::8192:56bb/64
```

BEISPIEL 11–10 Konfiguration eines 6to4-Tunnels mithilfe des Befehls `ifconfig` (Kurzform)

Das folgende Beispiel zeigt die Kurzform für die Konfiguration eines 6to4-Tunnels:

```
# ifconfig ip.6to4tun0 inet6 plumb
# ifconfig ip.6to4tun0 inet tsrc 129.146.86.187 up

# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NONUD,IPv6>mtu 1480 index 11
        inet tunnel src 129.146.86.187
        tunnel hop limit 60
        inet6 2002:8192:56bb::1/64
```

Änderungen an einem `netstat`-Befehl zur Unterstützung von IPv6

Der Befehl `netstat` zeigt sowohl den IPv4- als auch den IPv6-Netzwerkstatus an. Setzen Sie den Wert `DEFAULT_IP` in der Datei `/etc/default/inet_type`, um auszuwählen, welche Protokollinformationen angezeigt werden. Alternativ können Sie hierzu die Befehlszeilenoption `-f` verwenden. Mit einer permanenten Einstellung von `DEFAULT_IP` können Sie sicherstellen, dass `netstat` nur IPv4-Informationen anzeigt. Diese Einstellung können Sie durch die Option `-f` außer Kraft setzen. Weitere Informationen zur `inet_type`-Datei finden Sie in der Manpage `inet_type(4)`.

Mit der Option `-p` des Befehls `netstat` zeigen Sie die net-to-media-Tabelle an, die ARP-Tabelle für IPv4 und den Neighbor-Cache für IPv6. Weitere Informationen finden Sie in der Manpage `netstat(1M)` Unter „So zeigen Sie den Status der Sockets an“ auf Seite 229 finden Sie Beschreibungen von Verfahren, die diesen Befehl verwenden.

Änderungen an einem `snoop`-Befehl zur Unterstützung von IPv6

Mit dem Befehl `snoop` können Sie sowohl IPv4- als auch IPv6-Pakete erfassen. Dieser Befehl kann IPv6-Header, IPv6-Extension-Header, ICMPv6-Header und Neighbor Discovery-Protokolldaten anzeigen. Standardmäßig zeigt der Befehl `snoop` sowohl IPv4- als auch IPv6-Pakete an. Wenn Sie das Protokollschlüsselwort `ip` oder `ip6` angeben, zeigt der Befehl `snoop` nur IPv4- bzw. IPv6-Pakete an. Mit der IPv6-Filteroptionen können Sie alle

Pakete (sowohl IPv4 als auch IPv6) filtern, um nur IPv6-Pakete anzuzeigen. Weitere Informationen finden Sie in der Manpage `snoop(1M)` Unter „So überwachen Sie den IPv6-Netzwerkverkehr“ auf Seite 241 finden Sie Verfahren, die den `snoop`-Befehl verwenden.

Änderungen an einem `route`-Befehl zur Unterstützung von IPv6

Der Befehl `route` kann sowohl an IPv4- als auch an IPv6-Routen angewendet werden; IPv4-Routen sind dabei die Standardeinstellung. Wenn Sie die Option `-inet6` direkt hinter dem Befehl `route` in die Befehlszeile eingegeben, werden die Vorgänge an IPv6-Routen durchgeführt. Weitere Informationen finden Sie in der Manpage `route(1M)`.

Änderungen an einem `ping`-Befehl zur Unterstützung von IPv6

Mit dem Befehl `ping` können sowohl IPv4- als auch IPv6-Protokolle zum Sondieren von Zielhosts verwendet werden. Die Protokollauswahl hängt von den Adressen ab, die vom Namensserver für den angegebenen Zielhost zurückgegeben werden. Standardmäßig verwendet der Befehl `ping` das IPv6-Protokoll, wenn der Namensserver eine IPv6-Adresse für den Zielhost zurückgibt. Gibt der Server nur eine IPv4-Adresse zurück, verwendet `ping` das IPv4-Protokoll. Sie können diese Option mit der Befehlszeilenoption `-A` außer Kraft setzen, indem Sie angeben, welches Protokoll verwendet werden soll.

Ausführliche Informationen finden Sie in der Manpage `ping(1M)` Verfahren, die den Befehl `ping` verwenden, finden Sie unter „Ermitteln des Status von Remote-Hosts mit dem Befehl `ping`“ auf Seite 232.

Änderungen an einem `traceroute`-Befehl zur Unterstützung von IPv6

Mit dem Befehl `traceroute` können Sie sowohl IPv4- als auch IPv6-Routen zu einem bestimmten Host verfolgen. Aus Sicht des Protokolls verwendet `traceroute` den gleichen Algorithmus wie `ping`. Verwenden Sie die Befehlszeilenoption `-A`, um diese Auswahl außer Kraft zu setzen. Mit der Befehlszeilenoption `-a` können Sie jede einzelne Route an jede Adresse eines Multihomed-Host verfolgen.

Ausführliche Informationen finden Sie in der Manpage `traceroute(1M)` Verfahren, die den Befehl `traceroute` verwenden, finden Sie unter „Anzeigen von Routing-Informationen mit dem Befehl `traceroute`“ auf Seite 237.

IPv6-bezogene Daemons

In diesem Abschnitt werden IPv4-bezogene Daemons beschrieben.

`in.ndpd`-Daemon zur Neighbor Discovery

Der `in.ndpd`-in Daemon implementiert das IPv6-Neighbor Discovery-Protokoll und die Router-Erkennung. Darüber hinaus setzt der Daemon die automatische Adresskonfiguration für IPv6 um. Im Folgenden sind die unterstützten Optionen des `in.ndpd`-Daemons aufgeführt.

`-d` Aktiviert das Debugging.

`-D` Aktiviert das Debugging für bestimmte Ereignisse.

`-f` Gibt eine Datei an, die anstelle der Standard-Datei `/etc/inet/ndpd.conf` zum Einlesen von Konfigurationsdaten verwendet wird.

`-I` Druckt Informationen zu jeder Schnittstelle.

`-n` Führt kein Loopback für Router Advertisement-Nachrichten aus.

`-r` Ignoriert empfangene Pakete.

`-v` Aktiviert den ausführlichen Modus und zeigt verschiedene Diagnosemeldungen an.

`-t` Aktiviert die Paketverfolgung.

Der `in.ndpd`-Daemon wird neben den Parametern, die in der Konfigurationsdatei `/etc/inet/ndpd.conf` eingerichtet werden, durch die entsprechenden Parameter in der Startdatei `/var/inet/ndpd_state.`*Schnittstelle* gesteuert.

Wenn die Datei `/etc/inet/ndpd.conf` vorhanden ist, wird sie geparst und zur Konfiguration eines Knotens als Router verwendet. Tabelle 11–2 enthält eine Liste der gültigen Schlüsselwörter, die in dieser Datei enthalten sein können. Wenn ein Host bootet, stehen die Router eventuell nicht sofort zur Verfügung. Vom Router gesendete Pakete werden eventuell abgeworfen. Eventuell erreichen gesendete Pakete den Host nicht.

Die `/var/inet/ndpd_state.`*Schnittstelle*-Datei ist eine Statusdatei. Diese Datei wird regelmäßig von jedem Knoten aktualisiert. Wenn ein Knoten ausfällt und neu gestartet wird, kann der Knoten seine Schnittstellen auch bei Abwesenheit von Routern konfigurieren. Diese Datei enthält die Schnittstellenadresse, das Datum der letzten Aktualisierung der Datei und den Gültigkeitszeitraum der Datei. Darüber hinaus enthält diese Datei weitere Parameter, die bei früheren Router Advertisement-Nachrichten „gelernt“ wurden.

Hinweis – Sie müssen die Inhalte von Statusdateien nicht ändern. Statusdateien werden automatisch vom `in.ndpd`-Daemon gepflegt.

Eine Liste der Konfigurationsvariablen sowie der zulässigen Werte finden Sie in den Manpages `in.ndpd`(1M)und `ndpd.conf`(4).

`in.ripngd`-Daemon, für das IPv6-Routing

Der `in.ripngd`-Daemon implementiert das Routing Information Protocol der nächsten Generation für IPv6-Router (RIPng). RIPng ist das IPv6-Äquivalent von RIP. Wenn Sie einen IPv6-Router mit dem Befehl `routeadm` konfigurieren und das IPv6-Routing aktivieren, implementiert der `in.ripngd`-Daemon RIPng auf dem Router.

Im Folgenden sind die von RIPng unterstützten Optionen aufgeführt.

`-p` *n* — *n* gibt den alternativen Port an, der zum Senden und Empfangen von RIPnG-Paketen verwendet wird.

`-q` — Unterdrückt Routing-Informationen.

`-s` — Erzwingt Routing-Informationen auch dann, wenn der Daemon als Router fungiert.

`-P` — Unterdrückt die Verwendung von Poison Reverse.

`-S` — Wenn `in.ripngd` nicht als Router fungiert, gibt der Daemon nur eine Standard-Route für jeden Router ein.

`inetd`-Daemon und IPv6-Services

Eine IPv6-konforme Serveranwendung kann sowohl IPv4- als auch IPv6-Anforderungen oder nur IPv6-Anforderungen verarbeiten. Der Server verarbeitet Anforderungen immer über einen IPv6-Socket. Darüber hinaus verwendet der Server das gleiche Protokoll wie der entsprechende Client. Um einen Service für IPv6 hinzuzufügen oder zu modifizieren, verwenden Sie die Befehle der Service Management Facility (SMF).

- Weitere Informationen zu den SMF-Befehlen finden Sie im „SMF Command-Line Administrative Utilities" in *System Administration Guide: Basic Administration*.
- Eine Beispielaufgabe, die SMF zur Konfiguration eines IPv4-Servicemanifestes verwendet, das über SCTP ausgeführt wird, finden Sie unter „So fügen Sie Services hinzu, die das SCTP-Protokoll verwenden" auf Seite 143.

Bei der Konfiguration eines IPv6-Services müssen Sie sicherstellen, dass der Feldwert `proto` im Profil `inetadm` den entsprechenden Wert für diesen Service enthält:

- Bei einem Service, der sowohl IPv4- als auch IPv6-Anforderungen verarbeitet, wählen Sie `tcp6`, `udp6` oder `sctp`. Ein `proto`-Wert von `tcp6`, `udp6` oder `sctp6` führt dazu, dass `inetd` einen IPv6-Socket an den Server übergibt. Der Server enthält eine IPv4-zugeordnete Adresse, falls ein IPv4-Client eine Anforderung stellt.
- Bei einem Service, der ausschließlich IPv6-Anforderungen verarbeitet, wählen Sie `tcp6only` oder `udp6only`. Wenn einer dieser Werte für `proto` eingerichtet wurde, übergibt `inetd` einen IPv6-Socket an den Server.

Wenn Sie einen Oracle Solaris-Befehl durch eine andere Implementierung ersetzen, müssen Sie sicherstellen, dass die Implementierung dieses Service IPv6 unterstützt. Andernfalls müssen Sie `tcp`, `udp` oder `sctp` als `proto`-Wert angeben

Im Folgenden finden Sie ein Profil, das aus der Ausführung von `inetadm` für ein `echo`-Servicemanifest resultiert, das sowohl IPv4 als auch IPv6 unterstützt und über SCTP ausgeführt wird:

```
# inetadm -l svc:/network/echo:sctp_stream
    SCOPE    NAME=VALUE      name="echo"
             endpoint_type="stream"
             proto="sctp6"
             isrpc=FALSE
             wait=FALSE
             exec="/usr/lib/inet/in.echod -s"
             user="root"
    default  bind_addr=""
    default  bind_fail_max=-1
    default  bind_fail_interval=-1
    default  max_con_rate=-1
    default  max_copies=-1
    default  con_rate_offline=-1
    default  failrate_cnt=40
    default  failrate_interval=60
    default  inherit_env=TRUE
    default  tcp_trace=FALSE
    default  tcp_wrappers=FALSE
```

Um den Wert des Feldes `proto` zu ändern, verwenden Sie die folgende Syntax:

```
# inetadm -m FMRI proto="transport-protocols"
```

Alle Server, auf denen die Oracle Solaris-Software installiert ist, benötigen nur einen Profileintrag, der `proto` als `tcp6`, `udp6` oder `sctp6` einrichtet. Der Remote Shell Server (`shell`) und der Remote Execution Server (`exec`) bestehen jetzt jedoch aus einer Service-Instanz, die einen `proto`-Wert benötigt, für den die beiden Werte `tcp` und `tcp6only` erforderlich sind. Um beispielsweise den Wert `proto` für `shell` einzurichten, geben Sie den folgenden Befehl ein:

```
# inetadm -m network/shell:default proto="tcp,tcp6only"
```

Weitere Informationen zum Schreiben von IPv4-konformen Servern, die Sockets verwenden, finden Sie in den IPv6-Erweiterungen zur Socket API im *Programming Interfaces Guide* .

Überlegungen bei der Konfiguration eines Services für IPv6

Wenn Sie einen Service für IPv6 hinzufügen oder modifizieren, müssen Sie Folgendes berücksichtigen:

- Sie müssen den `proto`-Wert als `tcp6`, `sctp6` oder `udp6` angeben, um sowohl IPv4- als auch IPv6-Verbindungen zu ermöglichen. Wenn Sie den Wert für `proto` mit `tcp`, `sctp` oder `udp` angeben, verwendet der Service ausschließlich IPv4.
- Obwohl Sie eine Service-Instanz hinzufügen können, die 1:n-SCTP-Sockets für `inetd` verwendet, wird diese Vorgehensweise nicht empfohlen. `inetd` arbeitet nicht mit 1:n-SCTP-Sockets.
- Wenn ein Service zwei Einträge erfordert, da seine `wait-status`- oder `exec`-Eigenschaften abweichen, müssen Sie zwei Instanzen/Services aus dem ursprünglichen Service erstellen.

IPv6 Neighbor Discovery-Protokoll

IPv6 führt das Neighbor Discovery-Protokoll ein (siehe RFC 2461, Neighbor Discovery for IP Version 6 (IPv6) (`http://www.ietf.org/rfc/rfc2461.txt?number=2461`)). Eine Übersicht der wichtigsten Funktionen des Neighbor Discovery-Protokolls finden Sie unter „Einführung in das IPv6 Neighbor Discovery-Protokoll" auf Seite 84.

In diesem Abschnitt werden die folgenden Funktionen des Neighbor Discovery-Protokolls beschrieben:

- „ICMP-Nachrichten im Neighbor Discovery-Protokoll" auf Seite 299
- „Automatische Konfiguration" auf Seite 300
- „Neighbor Solicitation und Unerreichbarkeit" auf Seite 302
- „Algorithmus zur Erkennung doppelt vorhandener Adressen" auf Seite 303
- „Vergleich von Neighbor Discovery mit ARP und verwandten IPv4-Protokollen" auf Seite 304

ICMP-Nachrichten im Neighbor Discovery-Protokoll

Das Neighbor Discovery-Protokoll definiert fünf neue Internet Control Message Protocol (ICMP)-Nachrichten. Diese Nachrichten haben die folgenden Aufgaben:

- **Router Solicitation** – Nachdem eine Schnittstelle aktiviert wurde, können Hosts so genannte Router Solicitation-Nachrichten senden. Die Solicitation-Nachrichten fordern Router auf, sofort und nicht erst zur nächsten geplanten Zeit Router Advertisement-Nachrichten zu erzeugen.
- **Router Advertisement** – Router geben ihr Vorhandensein, verschiedene Link-Parameter und verschiedene Internet-Parameter bekannt. Sie senden diese Advertisement-Nachrichten entweder regelmäßig oder als Reaktion auf eine Router Solicitation-Nachricht. Router Advertisement-Nachrichten können Präfixe enthalten, die zur On-Link-Feststellung oder Adresskonfiguration, einem vorgeschlagenen Grenzwert für Hops usw. verwendet werden können.

- **Neighbor Solicitation** – Knoten senden Neighbor Solicitation-Nachrichten, um die Sicherungsschichtadresse eines Nachbarknotens zu ermitteln. Neighbor Solicitation-Nachrichten dienen auch dazu, um festzustellen, ob ein Nachbarknoten noch immer über eine zwischengespeicherte Sicherungsschichtadresse erreichbar ist. Neighbor Solicitations-Nachrichten werden auch zur Erkennung doppelt vorhandener Adressen verwendet.
- **Neighbor Advertisement** – Ein Knoten sendet Neighbor Advertisement-Nachrichten als Reaktion auf eine Neighbor Solicitation-Nachricht. Der Knoten kann auch unaufgeforderte Neighbor Advertisement-Nachrichten senden, um eine Änderung der Sicherungsschichtadresse bekannt zu geben.
- **Redirect** – Router verwenden Redirect-Nachrichten, um Hosts über einen besseren ersten Hop zu einem Ziel zu informieren, oder darüber, dass sich das Ziel auf dem gleichen Link befindet.

Automatische Konfiguration

Dieser Abschnitt enthält eine Übersicht der Schritte, die normalerweise bei einer automatischen Konfiguration einer Schnittstelle ausgeführt werden. Die automatische Konfiguration wird nur bei Multicast-konformen Links durchgeführt.

1. Einem Multicast-konforme Schnittstelle wird beispielsweise während des Systemstarts auf einem Knoten aktiviert.
2. Der Knoten beginnt die automatische Konfiguration durch Erzeugen einer Link-lokalen Adresse für die Schnittstelle.

   Die Link-lokale Adresse wird aus der Media Access Control (MAC)-Adresse der Schnittstelle gebildet.
3. Der Knoten sendet eine Neighbor Solicitation-Nachricht, die die vorläufige Link-lokale Adresse als Ziel enthält.

   Über diese Nachricht soll überprüft werden, ob die künftige Adresse nicht bereits von einem anderen Knoten in der Verknüpfung verwendet wird. Nach dieser Überprüfung kann die Link-lokale Adresse einer Schnittstelle zugewiesen werden.

   a. Wird die vorgeschlagene Adresse bereits von einem anderen Knoten verwendet, gibt dieser Knoten eine Neighbor Advertisement-Nachricht aus, dass diese Adresse bereits verwendet wird.

   b. Falls ein anderer Knoten ebenfalls versucht, diese Adresse zu verwenden, so sendet der Knoten eine Neighbor Solicitation-Nachricht für das Ziel.

      Die Anzahl der Neighbor Solicitation-Nachrichten oder -Neuübertragungen sowie die Verzögerung zwischen aufeinander folgenden Nachrichten sind Link-spezifisch. Sie können diese Parameter gegebenenfalls einstellen.

4. Wenn ein Knoten feststellt, dass die gewünschte Link-lokale Adresse nicht einmalig ist, wird die automatische Konfiguration angehalten. In diesem Fall müssen Sie die Link-lokale Adresse der Schnittstelle manuell konfigurieren.

   Um die Wiederherstellung zu vereinfachen, können Sie eine alternative Schnittstellen-ID angeben, mit der die Standardbezeichnung außer Kraft gesetzt wird. Dann kann die automatische Konfiguration mit der neuen, vermutlich einmaligen Schnittstellen-ID fortgesetzt werden.
5. Stellt ein Knoten fest, dass die potentielle Link-lokale Adresse einmalig ist, weist er diese Adresse der Schnittstelle zu.

   Jetzt verfügt der Knoten über Konnektivität auf IP-Ebene mit den benachbarten Knoten. Die verbleibenden Schritte bei der automatischen Konfiguration werden nur von Hosts durchgeführt.

Beziehen einer Router Advertisement-Nachricht

Die nächste Phase bei der automatischen Konfiguration ist das Beziehen einer Router Advertisement-Nachricht, es sei denn, es wird festgestellt, dass keine Router vorhanden sind. Wenn Router vorhanden sind, senden diese Router Advertisement-Nachrichten mit Angaben, welche Art einer automatischen Konfiguration ein Host ausführen soll.

Router senden die Router Advertisement-Nachrichten in regelmäßigen Abständen. Dennoch ist die Verzögerung zwischen aufeinander folgenden Advertisement-Nachrichten im Allgemeinen länger als ein Host, der eine automatische Konfiguration durchführt, warten kann. Um eine Advertisement-Nachricht schnell zu beziehen, sendet ein Host mindestens eine Router Solicitation-Nachricht an die Multicast-Gruppe „Alle-Router“.

Präfix-Konfigurationsvariablen

Neben anderen Informationen enthalten Router Advertisement-Nachrichten Präfixvariablen mit Daten, die von der statusfreien automatischen Adresskonfiguration zum Erzeugen von Präfixen verwendet werden. Das Feld „Stateless Address Autoconfiguration“ in Router Advertisement-Nachrichten wird unabhängig verarbeitet. Ein Optionsfeld mit Präfix-Daten, das Flag „Address Autoconfiguration“, gibt an, ob die Option auch für die statusfreie automatische Konfiguration gilt. Wird das Optionsfeld übernommen, können zusätzliche Optionsfelder ein Teilnetzpräfix mit Werten für die Lebensdauer enthalten. Diese Werte geben die Zeit an, über die Adressen, die aus dem Präfix erstellt wurden, priorisi Priorität genießen und gültig bleiben.

Da Router regelmäßig Router Advertisement-Nachrichten erzeugen, empfangen Hosts ständig neue Advertisements. IPv6-konforme Hosts verarbeiten die Informationen, die in den Advertisement-Nachrichten enthalten sind. Diese Informationen werden von den Hosts hinzugefügt. Darüber hinaus aktualisieren sie Informationen, die sie in vorherigen Advertisement-Nachrichten empfangen haben.

Einmaligkeit einer Adresse

Aus Sicherheitsgründen müssen alle Adressen auf Einmaligkeit geprüft werden, bevor sie einer Schnittstelle zugewiesen werden. Bei Adressen, die über die statusfreie automatische Konfiguration erzeugt wurden, ist die Situation anders. Die Einmaligkeit einer Adresse wird vielmehr durch die Komponente der Adresse ermittelt, die aus der Schnittstellen-ID gebildet wird. Wenn also ein Knoten die Einmaligkeit einer Link-lokale Adresse bereits geprüft hat, müssen zusätzliche Adressen nicht mehr einzeln überprüft werden. Die Adressen müssen aus der gleichen Schnittstellen-ID erstellt werden. Im Gegensatz dazu müssen alle manuell bezogenen Adressen einzeln auf Einmaligkeit geprüft werden. Einige Systemadministratoren sind der Meinung, dass der zusätzliche Aufwand für die Erkennung doppelt vorhandener Adressen die Vorteile nicht aufwiegt. An diesen Standorten kann die Erkennung doppelt vorhandener Adressen deaktiviert werden, indem ein Konfiguration-Flag für jede Schnittstelle eingerichtet wird.

Um die automatische Konfiguration zu beschleunigen, kann ein Host seine Link-lokale Adresse selbst erzeugen und die Einmaligkeit sicherstellen, während der Host auf eine Router Advertisement-Nachricht wartet. Ein Router kann eine Antwort auf eine Router Solicitation-Nachricht um wenige Sekunden verzögern. Entsprechend kann die gesamte Zeit bis zum Abschluss einer automatischen Konfiguration länger sein, wenn die zwei Schritte nacheinander ausgeführt werden.

Neighbor Solicitation und Unerreichbarkeit

Das Neighbor Discovery verwendet *Neighbor Solicitation*-Nachrichten, um festzustellen, ob mehreren Knoten die gleiche Unicast-Adresse zugewiesen wurde. Die *Neighbor Unreachability Detection* stellt den Ausfall eines Nachbarknotens oder den Ausfall eines Weiterleitungspfads zu einem Nachbarknoten fest. Sie fordert eine positive Bestätigung, dass Pakete, die an einen Nachbarn gesendet wurden, auch tatsächlich empfangen wurde. Darüber hinaus stellt die Neighbor Unreachability Detection fest, ob Datenpakete von der IP-Schicht des Nachbarknotens ordnungsgemäß verarbeitet wurden.

Die Neighbor Unreachability Detection verwendet Bestätigungen aus zwei Quellen: Protokollen der oberen Schichten und Neighbor Solicitation-Nachrichten. Wenn möglich, bestätigen die Protokolle der oberen Schichten, dass Datenpakete über eine Verbindung *weitergeleitet* werden. Wenn beispielsweise neue TCP-Bestätigungen empfangen wurden, wird bestätigt, dass die zuvor gesendeten Daten korrekt empfangen wurden.

Empfängt ein Knoten keine positive Bestätigung von den Protokollen der oberen Schichten, sendet er unicast Neighbor Solicitation-Nachrichten. Diese Nachrichten fordern Neighbor Advertisement-Nachrichten zur Bestätigung der Erreichbarkeit vom nächsten Hop. Um unnötigen Netzwerkverkehrs zu verhindern, werden diese Sondierungsnachrichten nur an Nachbarknoten gesendet, an die der Knoten aktiv Pakete sendet.

Algorithmus zur Erkennung doppelt vorhandener Adressen

Um sicherzustellen, dass alle konfigurierten Adressen auf einer bestimmten Verknüpfung einmalig sind, wird ein Algorithmus zur *Erkennung doppelt vorhandener Adressen* an den Adressen ausgeführt. Die Knoten müssen den Algorithmus anwenden, bevor die Adressen einer Schnittstelle zugewiesen werden. Der Algorithmus zur Erkennung doppelt vorhandener Adressen wird an allen Adressen angewendet.

Die in diesem Abschnitt beschriebene automatische Konfiguration gilt nur für Hosts und nicht für Router. Da die automatische Hostkonfiguration Daten verwendet, die von Routern bekannt gegeben werden, müssen Router auf andere Weise konfiguriert werden. Router erzeugen Link-lokale Adressen mithilfe eines Mechanismus, auf den in diesem Kapitel noch näher eingegangen wird. Darüber hinaus wird von Routern erwartet, dass sie den Algorithmus zur Erkennung doppelt vorhandener Adressen erfolgreich abschließen, bevor sie eine Adresse einer Schnittstelle zuweisen.

Proxy Advertisement-Nachrichten

Ein Router, der im Auftrag einer Zieladresse Pakete akzeptiert, kann nicht-überschreibende Neighbor Advertisement-Nachrichten ausgeben. Der Router kann Pakete für eine Zieladresse annehmen, die nicht in der Lage ist, selbst auf Neighbor Solicitation-Nachrichten zu reagieren. Derzeit ist die Verwendung eines Proxy nicht vorgegeben. Proxy-Advertisement-Nachrichten können jedoch verwendet werden, wenn mobile Knoten nicht mit der Verknüpfung verbunden sind. Beachten Sie, dass die Verwendung eines Proxy nicht als allgemeiner Mechanismus zur Arbeit mit Knoten vorgesehen ist, die dieses Protokoll nicht implementieren.

Lastausgleich für eingehende Daten

Knoten mit replizierten Schnittstellen müssen eventuell einen Lastausgleich beim Empfang eingehender Datenpakete über mehrere Netzwerkschnittstellen auf dem gleichen Link durchführen. Solche Knoten verfügen über Link-lokale Adressen, die der gleichen Schnittstelle zugeordnet sind. Beispielsweise kann ein einzelner Netzwerktreiber mehrere Netzwerkschnittstellenkarten als eine einzelne logische Schnittstelle mit mehreren Link-lokalen Adressen darstellen.

Der Lastausgleich erfolgt, indem Router die Link-lokale Quelladresse aus den Router Advertisement-Paketen weglassen. Folglich müssen Nachbarknoten Neighbor Solicitation-Nachrichten verwenden, um die Link-lokalen Adressen der Router zu lernen. Zurückgelieferte Neighbor Advertisement-Meldungen können dann Link-lokale Adressen enthalten, die je nachdem, wer die Solicitation veranlasst hat, unterschiedlich sind.

Ändern einer Link-lokalen Adresse

Ein Knoten, der sich der Änderung seiner Link-lokalen Adresse bewusst ist, kann unaufgefordert Multicast Neighbor Advertisement-Pakete senden. Der Knoten kann Multicast-Pakete an alle Knoten senden, um die ungültig gewordenen Link-lokalen Adressen in den Cache-Speichern zu aktualisieren. Das Senden unaufgeforderter Advertisement-Nachrichten dient ausschließlich zur Leistungsverbesserung. Der Algorithmus zur Neighbor Unreachability-Erkennung stellt sicher, dass alle Knoten die neue Adresse zuverlässig erkennen, obwohl die Verzögerung etwas größer sein könnte.

Vergleich von Neighbor Discovery mit ARP und verwandten IPv4-Protokollen

Die Funktionen des IPv6-Neighbor Discovery-Protokolls entsprechen einer Kombination der folgenden IPv4-Protokolle: Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery und ICMP Redirect. IPv4 verfügt jedoch nicht über ein allgemein anerkanntes Protokoll oder einen Mechanismus zur Neighbor Unreachability-Erkennung. Die Host-Anforderungen geben jedoch einige mögliche Algorithmen zur Dead Gateway-Erkennung vor. Die Dead Gateway-Erkennung ist Teil der Probleme, die mit der Neighbor Unreachability-Erkennung gelöst werden.

In der folgenden Liste wird das Neighbor Discovery-Protokoll mit dem entsprechenden Satz an IPv4-Protokollen verglichen.

- Die Router-Erkennung ist Teil des allgemeinen IPv6-Protokollsatzes. IPv6-Hosts benötigen keinen `snoop`-Befehl für die Routing-Protokolle, um einen Router zu finden. IPv4 verwendet ARP, ICMP Router-Erkennung und ICMP-Redirect zur Router-Erkennung.
- IPv6-Router Advertisement-Nachrichten übertragen Link-lokale Adressen. Zum Auflösen der Link-lokalen Adresse des Routers müssen keine zusätzlichen Pakete ausgetauscht werden.
- Router Advertisement-Nachrichten übertragen die Standortpräfixe eines Links. Zur Konfiguration der Netzmaske ist kein separater Mechanismus erforderlich, wie dies bei IPv4 der Fall ist.
- Router Advertisement-Nachrichten ermöglichen eine automatische Addresskonfiguration. Die automatische Konfiguration ist in IPv4 nicht implementiert.
- Das Neighbor Discovery-Protokoll ermöglicht es IPv6-Routern, eine für den Link geltende MTU für Hosts bekannt zu geben. Entsprechend verwenden alle Knoten den gleichen MTU-Wert auf Links, für die keine MTU definiert wurde. IPv4-Hosts im gleichen Netzwerk können unterschiedliche MTUs aufweisen.

- Im Gegensatz zu IPv4-Broadcast-Adressen sind IPv6-Adressauflösung-Multicasts über 4 (2^32) Milliarden Multicast-Adressen verteilt, wodurch aufgrund der Adressauflösung auftretende Unterbrechungen auf Knoten, bei denen es sich nicht um das Ziel handelt, wesentlich reduziert werden. Darüber hinaus sollten nicht-IPv6-Computer überhaupt nicht unterbrochen werden.
- IPv6-Redirects enthalten die Link-lokale Adresse des neuen ersten Hop. Eine separate Adressauflösung ist nach dem Empfang einer Umleitung (Redirect) nicht mehr erforderlich.
- Einem IPv6-Netzwerk können mehrere Standortpräfixe zugewiesen werden. Standardmäßig lernen alle lokalen Standortpräfixe aus den Router Advertisement-Nachrichten. Router können jedoch auch so konfiguriert werden, dass einige oder alle Präfixe in Router Advertisement-Nachrichten weggelassen werden. In diesen Fällen nehmen Hosts an, dass sich die Ziele in Remote-Netzwerken befinden. Entsprechend senden sie den Datenverkehr an Router. Ein Router kann dann gegebenenfalls Umleitungen initiieren.
- Im Gegensatz zu IPv4 geht der Empfänger einer IPv6-Redirect-Nachricht davon aus, dass sich der nächste Hop im lokalen Netzwerk befindet. Unter IPv4 ignoriert ein Host Redirect-Nachrichten, in denen angegeben wird, dass sich ein nächster Hop entsprechend der Netzwerkmaske nicht im lokalen Netzwerk befindet. Der IPv6-Redirect-Mechanismus ist analog der XRedirect-Funktion in IPv4. Der Redirect-Mechanismus eignet sich für nicht-Broadcast- und gemeinsam genutzte Media-Links. In diesen Netzwerken sollen Knoten nicht auf alle Präfixe für Ziele auf dem lokalen Link prüfen.
- Die Neighbor Unreachability Detection unter IPv6 verbessert die Paketzustellung bei fehlerhaften Routern. Diese Funktion verbessert die Paketzustellung bei teilweise fehlerhaften oder partitionierten Links. Darüber hinaus verbessert diese Funktion die Paketzustellung über Knoten, deren Link-lokale Adressen geändert wurden. Beispielsweise können mobile Knoten aus dem lokalen Netzwerk verschoben worden sein, ohne dass sie aufgrund veralteter ARP-Caches die Konnektivität verlieren. IPv4 verfügt über keine entsprechende Methode zur Neighbor Unreachability Detection.
- Im Gegensatz zu ARP erfasst das Neighbor Discovery-Protokoll Half-Link-Ausfälle mithilfe der Neighbor Unreachability Detection. Das Neighbor Discovery-Protokoll vermeidet das Senden von Datenverkehr an Nachbarknoten, wenn keine doppelseitige Konnektivität vorhanden ist.
- IPv6-Hosts können die Router-Assoziationen mithilfe von Link-lokalen Adressen pflegen, um Router eindeutig zu identifizieren. Die Fähigkeit zur Identifizierung von Routern ist für Router Advertisement- und Redirect -Nachrichten erforderlich. Hosts müssen Router-Assoziationen pflegen, wenn globale Präfixe am Standort verwendet werden. IPv4 verfügt über keine vergleichbare Methode zur Identifizierung von Routern.

- Da Neighbor Discovery-Nachrichten nach dem Empfang auf maximal 255 Hops beschränkt sind, ist das Protokoll immun gegenüber Spoofing-Angriffen, die von Knoten außerhalb des Links stammen. Im Gegensatz dazu können IPv4-Knoten außerhalb des Links ICMP-Redirect-Nachrichten senden. IPv4-Knoten außerhalb des Links können auch Router Advertisement-Nachrichten senden.
- Durch Ausführen der Adressauflösung auf der ICMP-Schicht wird das Neighbor Discovery-Protokoll weniger von Medien abhängig als das ARP. Entsprechend können standardmäßige IP-Authentifizierungs- und Sicherheitsmechanismen verwendet werden.

IPv6-Routing

Routing unter IPv6 ist nahezu identisch mit dem IPv4-Routing unter Classless Inter-Domain Routing (CIDR). Der einzige Unterschied besteht darin, dass es sich bei den Adressen um 128-Bit-IPv6-Adressen anstelle von 32-Bit-IPv4-Adressen handelt. Bei sehr einfachen Erweiterungen können alle IPv4-Routing-Algorithmen, z. B. OSPF, RIP, IDRP und IS-IS, zum Routen von IPv6 verwendet werden.

Darüber hinaus bietet IPv6 einfache Routing-Erweiterungen, die mächtige neue Routing-Funktionen unterstützen. Die neuen Routing-Funktionen sind in der folgenden Liste aufgeführt:

- Provider-Auswahl basierend auf Richtlinie, Leistung, Kosten usw.
- Host-Mobilität, Route zum aktuellen Standort
- Automatische Neuadressierung, Route zur neuen Adresse

Sie beziehen die neuen Routing-Funktionen, indem Sie Sequenzen von IPv6-Adressen erstellen, die eine IPv6-Routing-Option verwenden. Eine IPv6-Quelle verwendet die Routing-Option, um einen oder mehrere Zwischenknoten oder topologische Gruppen auf dem Pfad zum Datenpaketziel aufzulisten. Diese Funktion ähnelt der IPv4-Option „Loose Source and Record Route“ (LSRR).

Um Adresssequenzen in eine allgemeine Funktion umzuwandeln, müssen IPv6-Hosts in den meisten Fällen die Routen in einem vom Host empfangenen Paket umkehren. Das Paket muss mithilfe des IPv6-Authentifizierung-Header erfolgreich authentifiziert worden sein. Das Paket muss Adresssequenzen enthalten, damit es an den Absender zurückgesendet werden kann. Diese Technik macht es erforderlich, dass IPv6-Host-Implementierungen die Verarbeitung und Umkehrung von Quellrouten unterstützen. Verarbeitung und Umkehrung von Quellrouten ermöglichen es einem Provider, mit Hosts zu arbeiten, die neue IPv6-Funktionen wie Provider-Auswahl und erweiterte Adressen verwenden.

Router Advertisement-Nachrichten

Bei Multicast-fähigen Links und Point-to-Point-Links sendet jeder Router in regelmäßigen Abständen ein Router Advertisement-Paket an die Multicast-Gruppe, in der er seine Verfügbarkeit bekannt gibt. Ein Host empfängt Router Advertisement-Nachrichten von allen Routern und erstellt so eine Liste der Standard-Router. Router erzeugen diese Router Advertisement-Nachrichten so häufig, dass Hosts innerhalb weniger Minuten über das Vorhandensein von Routern informiert sind. Dennoch erfolgen diese Nachrichten nicht häufig genug, um den Ausfall eines Routers am Ausbleiben der Advertisement-Nachrichten zu erkennen. Eine zuverlässige Ausfallerkennung erfolgt über einen separaten Algorithmus, der die Unerreichbarkeit eines Nachbarknotens feststellt.

Router Advertisement-Präfixe

Router Advertisement-Nachrichten enthalten eine Liste der Teilnetzpräfixe, mit der festgestellt wird, ob sich ein Host auf dem gleichen Link (on-Link) wie der Router befindet. Die Präfixliste dient auch zur autonomen Adresskonfiguration. Präfixen zugeordnete Flags kennzeichnen, dass ein bestimmtes Präfix absichtlich verwendet wird. Hosts erstellen und verwalten anhand der bekannt gegebenen on-Link-Präfixe eine Liste mit Angaben, ob sich das Ziel eines Datenpakets on-Link oder hinter einem Router befindet. Ein Ziel kann auch dann on-Link sein, wenn es in keinem bekannt gegebenen on-Link-Präfix enthalten ist. In diesen Fällen kann ein Router eine Redirect-Nachricht senden. Die Redirect-Nachricht informiert den Absender, dass es sich bei dem Ziel um einen Nachbarknoten handelt.

Mit Router Advertisement-Nachrichten und Flags für jedes Präfix können Router Hosts darüber zu informieren, wie eine statusfreie automatische Adresskonfiguration durchgeführt wird.

Router Advertisement-Nachrichten

Router Advertisement-Nachrichten enthalten auch Internet-Parameter, z. B. einen Grenzwert für die Hops, den Hosts in abgehenden Paketen verwenden sollen. Optional enthalten Router Advertisement-Nachrichten auch Link-Parameter, z. B. die Link-MTU. Diese Funktion ermöglicht eine zentralisierte Verwaltung kritischer Parameter. Die Parameter können auf Routern eingerichtet und automatisch an alle angeschlossenen Hosts gesendet werden.

Knoten führen die Adressauflösung durch, indem eine Neighbor Solicitation-Nachricht an die Multicast-Gruppe gesendet wird. Sie fordert einen Zielknoten auf, seine Sicherungsschichtadresse zurückzusenden. Multicast Neighbor Solicitation-Nachrichten werden an die Solicited Node-Multicast-Adresse der Zieladresse gesendet. Das Ziel gibt seine Sicherungsschichtadresse als Unicast Neighbor Advertisement-Nachricht zurück. Ein einzelnes Anforderung/Antwort-Paketpaar reicht für den Initiator und das Ziel aus, die Sicherungsschichtadresse des jeweils anderen aufzulösen. Der Initiator sendet seine Sicherungsschichtadresse in der Neighbor Solicitation-Nachricht.

IPv6-Tunnel

Um die Abhängigkeiten an einem Dual-Stack IPv4/IPv6-Standort zu minimieren, müssen die Router im Pfad zwischen zwei IPv6-Knoten kein IPv6 unterstützen. Der Mechanismus, der eine solche Netzwerkkonfiguration unterstützt, wird als *Tunneling* bezeichnet. Im Grunde genommen werden IPv6-Pakete in IPv4-Pakete verpackt und dann über die IPv4-Router geleitet. Die folgende Abbildung verdeutlicht den Tunneling-Mechanismus über die IPv4-Router, die in der Abbildung durch „R“ gekennzeichnet sind

ABBILDUNG 11–5 IPv6-Tunneling-Mechanismus

Die Oracle Solaris IPv6-Implementierung verwendet zwei Arten von Tunneling-Mechanismen:

- Zwischen zwei Routern konfigurierte Tunnel (siehe Abbildung 11–5)
- Automatische Tunnel, die an den Endpunkt-Hosts terminiert sind

Ein konfigurierter Tunnel wird derzeit für verschiedene Zwecke im Internet verwendet, z. B. auf dem MBONE, dem IPv4-Multicast-Backbone. Im Prinzip besteht der Tunnel aus zwei Routern, die mit einer virtuellen Point-to-Point-Verbindung zwischen zwei Routern über das

IPv4-Netzwerk konfiguriert sind. Diese Art Tunnel wird wahrscheinlich in naher Zukunft in einigen Bereichen des Internet verwendet werden.

Automatische Tunnel erfordern IPv4-kompatible Adressen. Automatische Tunnel können zum Verbinden von IPv6-Knoten verwendet werden, wenn keine IPv6-Router zur Verfügung stehen. Diese Tunnel beginnen entweder an einem Dual-Stack-Host oder einem Dual-Stack-Router, indem eine automatische Tunneling-Netzwerkschnittstelle konfiguriert wird. Die Tunnel enden immer bei dem Dual-Stack-Host. Diese Tunnel stellen die IPv4-Zieladresse (den Endpunkt des Tunnels) dynamisch fest, indem sie die Adresse aus der IPv4-kompatiblen Zieladresse extrahieren.

Konfigurierte Tunnel

Tunneling-Schnittstellen weisen das folgende Format auf:

`ip.tun` *ppa*

ppa ist der physikalische Anschlusspunkt.

Beim Systemstart wird das Tunneling-Modul (`tun`) vom `ifconfig`-Befehl an den Anfang des IP gebracht, um eine virtuelle Schnittstelle zu erstellen. Dieser Vorgang wird durch das Erstellen der entsprechenden `hostname6.*`-Datei begleitet.

Angenommen, Sie erstellen einen Tunnel zum Einkapseln von IPv6-Paketen über ein IPv4-Netzwerk (IPv6-über-IPv4), so erstellen Sie eine Datei mit dem folgenden Namen:

```
/etc/hostname6.ip.tun0
```

Der Inhalt dieser Datei wird an den Befehl `ifconfig` übergeben, nachdem die Schnittstellen geplumbt (aktiviert) wurden. Der Inhalt wird zu den Parametern, die zur Konfiguration eines Point-to-Point-Tunnels erforderlich sind.

BEISPIEL 11–11 `hostname6.ip.tun0`-Datei für einen IPv6-über-IPv4-Tunnel

Im Folgenden finden Sie ein Beispiel für die Einträge in der `hostname6.ip.tun0`-Datei:

```
tsrc 10.10.10.23 tdst 172.16.7.19 up
addif 2001:db8:3b4c:1:5678:5678::2 up
```

In diesem Beispiel werden die IPv4-Quell- und Zieladressen als Token verwendet, um Link-lokale IPv6-Adressen automatisch zu konfigurieren. Diese Adressen sind Quelle und Ziel der Schnittstelle `ip.tun0.` Es sind zwei Schnittstellen konfiguriert. Die Schnittstelle `ip.tun0` sind konfiguriert. Eine logische Schnittstelle, `ip.tun0:1`, wurde ebenfalls konfiguriert. Die logische Schnittstelle besitzt die Quelle- und IPv6-Zieladressen, die durch den Befehl `addif` angegeben werden.

Wird das System im Multiuser-Modus gestartet, kann der Inhalt dieser Konfigurationsdateien ohne Änderungen an den Befehl`ifconfig` übergeben werden. Die Einträge in Beispiel 11–11 entsprechen Folgendem:

```
# ifconfig ip.tun0 inet6 plumb
# ifconfig ip.tun0 inet6 tsrc 10.0.0.23 tdst 172.16.7.19 up
# ifconfig ip.tun0 inet6 addif 2001:db8:3b4c:1:5678:5678::2 up
```

Das Folgende zeigt die Ausgabe des Befehls `ifconfig -a` für diesen Tunnel.

```
ip.tun0: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,
  NONUD,IPv6> mtu 1480 index 6
        inet tunnel src 10.0.0.23  tunnel dst 172.16.7.19
        inet6 fe80::c0a8:6417/10 --> fe80::c0a8:713
ip.tun0:1: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,NONUD,IPv6> mtu 1480
  index 5
        inet6 2001:db8:3b4c:1:5678:5678::2
```

Sie können weitere logische Schnittstellen konfigurieren, in dem Sie der Konfigurationsdatei unter Beachtung der folgenden Syntax weitere Zeilen hinzufügen:

```
addif IPv6-source IPv6-destination up
```

Hinweis – Wenn es sich bei einem der Tunnelenden um einen IPv6-Router handelt, der mindestens ein Präfix über den Tunnel bekannt gibt, sind keine `addif`-Befehle in den Tunnelkonfigurationsdateien erforderlich. Nur `tsrc` und `tdst` sind eventuell erforderlich, da alle anderen Adressen automatisch konfiguriert wurden.

In einigen Fällen müssen bestimmte Quellen- und Zieladressen auf dem lokalen Link für einen bestimmten Tunnel manuell konfiguriert werden. Ändern Sie die erste Zeile der Konfigurationsdatei, um diese Link-lokalen Adressen aufzunehmen. Die folgende Zeile ist ein Beispiel:

```
tsrc 10.0.0.23 tdst 172.16.7.19 fe80::1/10 fe80::2 up
```

Bitte beachten Sie, das die Link-lokale Quellenadresse die·Präfixlänge 10 besitzt. In diesem Beispiel ähnelt die Schnittstelle `ip.tun0` Folgendem:

```
ip.tun0: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,NONUD,IPv6> mtu 1480
index 6
        inet tunnel src 10.0.0.23  tunnel dst 172.16.7.19
        inet6 fe80::1/10 --> fe80::2
```

Um einen Tunnel zum Einkapseln von IPv6-Paketen über ein IPv6-Netzwerk (IPv6-über-IPv6) zu erstellen, legen Sie die folgende Datei an:

```
/etc/hostname6.ip6.tun0
```

BEISPIEL 11–12 `hostname6.ip6.tun0`-Datei für einen IPv6-über-IPv6-Tunnel

Das Folgende ist ein Beispiel für die Einträge in der `hostname6.ip6.tun0`-Datei zur IPv6-Einkapselung über ein IPv6-Netzwerk:

```
tsrc 2001:db8:3b4c:114:a00:20ff:fe72:668c
        tdst 2001:db8:15fa:25:a00:20ff:fe9b:a1c3
fe80::4 fe80::61 up
```

Um einen Tunnel zum Einkapseln von IPv4-Paketen über ein IPv6-Netzwerk (IPv4-über-IPv6) zu erstellen, legen Sie die folgende Datei an:

```
/etc/hostname.ip6.tun0
```

BEISPIEL 11–13 `hostname.ip6.tun0`-Datei für einen IPv4-über-IPv6-Tunnel

Das Folgende ist ein Beispiel für die Einträge in der `hostname.ip6.tun0`-Datei zur IPv4-Einkapselung über ein IPv6-Netzwerk:

```
tsrc 2001:db8:3b4c:114:a00:20ff:fe72:668c
         tdst 2001:db8:15fa:25:a00:20ff:fe9b:a1c3
10.0.0.4 10.0.0.61 up
```

Um einen Tunnel zum Einkapseln von IPv4-Paketen über ein IPv4-Netzwerk (IPv4-über-IPv4) zu erstellen, legen Sie die folgende Datei an:

```
/etc/hostname.ip.tun0
```

BEISPIEL 11–14 `hostname.ip.tun0`-Datei für einen IPv4-über-IPv4-Tunnel

Das Folgende ist ein Beispiel für die Einträge in der `hostname.ip.tun0`-Datei zur IPv4-Einkapselung über ein IPv4-Netzwerk:

```
tsrc 172.16.86.158 tdst 192.168.86.122
10.0.0.4 10.0.0.61 up
```

Weitere Informationen zu `tun` finden Sie in der Manpage `tun`(7M). Eine allgemeine Beschreibung der Tunneling-Konzepte während des Übergangs zu IPv6 finden Sie unter „Einführung in IPv6-Tunnel“ auf Seite 87. Eine Beschreibung der Verfahren zur Konfiguration von Tunneln finden Sie unter „Aufgaben bei der Konfiguration von Tunneln zur Unterstützung von IPv6 (Übersicht der Schritte)“ auf Seite 204.

Automatische 6to4-Tunnel

Oracle Solaris bietet 6to4-Tunnel als bevorzugte Zwischenlösung für den Übergang von der IPv4- zur IPv6-Adressierung. Mit 6to4-Tunneln können isolierte IPv6-Standorte durch einen automatischen Tunnel über ein IPv4-Netzwerk, das IPv6 nicht unterstützt, miteinander kommunizieren. Zum Verwenden von 6to4-Tunneln müssen Sie einen Grenzrouter in Ihrem IPv6-Netzwerk als einen Endpunkt eines automatischen 6to4-Tunnels konfigurieren. Dann kann der 6to4-Router an einem Tunnel zu einem anderen IPv6-Standort, oder, falls erforderlich, mit einem nativen IPv6-, nicht-6to4-Standort teilnehmen.

In diesem Abschnitt finden Sie Referenzen zu den folgenden 6to4-bezogenen Themen:

- Topologie eines 6to4-Tunnels
- 6to4-Adressierung, einschließlich Format der Advertisement-Nachricht
- Beschreibung des Paketflusses durch einen 6to4-Tunnel
- Topologie eines Tunnels zwischen einem 6to4-Router und einem 6to4-Relay-Router
- Vor der Konfiguration einer 6to4-Relay-Router-Unterstützung zu berücksichtigende Aspekte

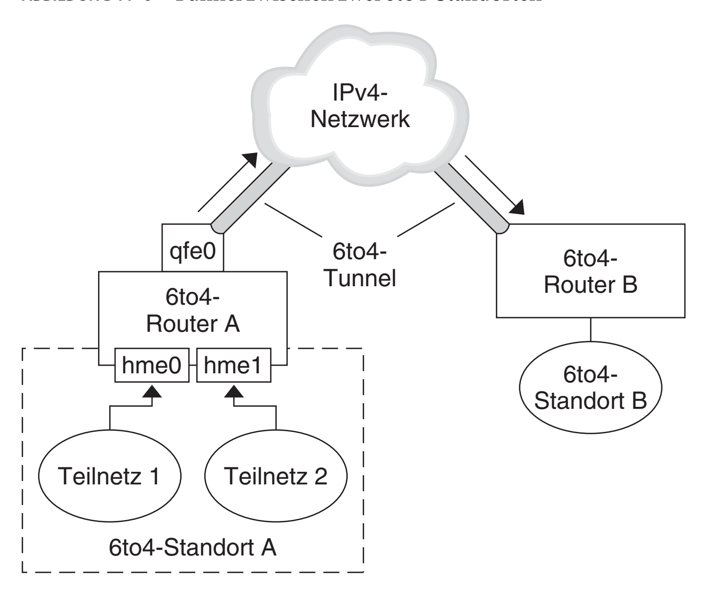
In der folgenden Tabelle sind zusätzliche Aufgaben zum Konfigurieren von 6to4-Tunneln aufgeführt, sowie Ressourcen zur Beschaffung weiterer hilfreicher Informationen.

Aufgabe oder Detail	Weitere Informationen
Aufgaben bei der Konfiguration eines 6to4-Tunnels	„So konfigurieren Sie einen 6to4-Tunnel" auf Seite 208
6to4-bezogene RFC	RFC 3056, „Connection of IPv6 Domains via IPv4 Clouds" (`http://www.ietf.org/rfc/rfc3056.txt`)
Ausführliche Informationen zum `6to4relay`-Befehl, der die Unterstützung von Tunneln zu einem 6to4-Relay-Router ermöglicht	`6to4relay`(1M)
6to4-Sicherheitsaspekte	Security Considerations for 6to4 (`http://www.ietf.org/rfc/rfc3964.txt`)

Topologie eines 6to4-Tunnels

Ein 6to4-Tunnel bietet IPv6-Konnektivität zu allen 6to4-Standorten weltweit. Entsprechend funktioniert der Tunnel auch als eine Verbindung zu allen IPv6-Standorten (einschließlich dem nativen IPv6-Internet), vorausgesetzt, der Tunnel ist zum Weiterleiten an einen Relay-Router konfiguriert. Die folgende Abbildung zeigt, wie ein 6to4-Tunnel diese Konnektivität zwischen zwei 6to4-Standorten bereitstellt.

ABBILDUNG 11–6 Tunnel zwischen zwei 6to4-Standorten



Die Abbildung zeigt zwei voneinander isolierte 6to4-Netzwerke, Standort A und Standort B. Jeder Standort ist mit einem Router konfiguriert, der über eine externe Verbindung zu einem IPv4-Netzwerk verfügt. Ein 6to4-Tunnel durch das IPv4-Netzwerk stellt eine Verbindung zu 6to4-Standorten bereit.

Bevor ein IPv6-Standort zu einem 6to4-Standort werden kann, muss mindestens eine Router-Schnittstelle zur Unterstützung von 6to4 konfiguriert werden. Diese Schnittstelle muss die externe Verbindung mit dem IPv4-Netzwerk bieten. Die Adresse, die Sie auf `qfe0` konfigurieren, muss global einmalig sein. In dieser Abbildung stellt die Schnittstelle `qfe0` des Grenzrouters A die Verbindung von Standort A mit dem IPv4-Netzwerk her. Die Schnittstelle `qfe0` muss bereits mit einer IPv4-Adresse konfiguriert worden sein, bevor Sie `qfe0` als eine 6to4-Pseudoschnittstelle konfigurieren.

In der Abbildung besteht der 6to4-Standort A aus zwei Teilnetzen, die über die Schnittstellen `hme0` und `hme1` auf Router A verbunden sind. Alle IPv6-Hosts in einem der Teilnetze von Standort A werden nach dem Empfang der Advertisement-Nachricht von Router A automatisch mit 6to4-abgeleiteten Adressen neu konfiguriert.

Standort B ist ein weiterer isolierter 6to4-Standort. Um Datenverkehr korrekt von Standort A zu empfangen, muss ein Grenzrouter an Standort B zur 6to4-Unterstützung konfiguriert sein. Andernfalls werden die Pakete, die der Router von Standort A empfängt, nicht erkannt und abgeworfen.

Paketfluss durch den 6to4-Tunnel

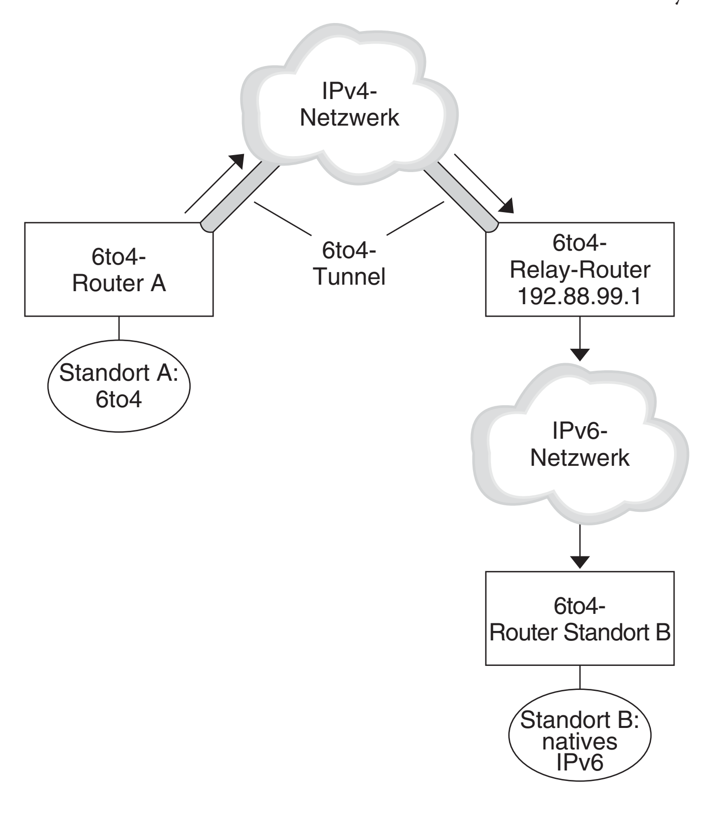
In diesem Abschnitt wird der Paketfluss von einem Host an einem 6to4-Standort zu einem Host an einem remoten 6to4-Standort beschrieben. Das Szenario verwendet die in Abbildung 11–6 gezeigte Topologie. Darüber hinaus wird bei diesem Szenario davon ausgegangen, dass die 6to4-Router und die -Hosts bereits konfiguriert sind.

1. Ein Host im Teilnetz 1 des 6to4-Standorts A sendet eine Übertragung mit einem Host am 6to4-Standort B als Ziel. Jeder Paket-Header enthält eine 6to4-abgeleitete Quelladresse und eine 6to4-abgeleitete Zieladresse.
2. Der Router an Standort A kapselt jedes 6to4-Datenpaket in einen IPv4-Header ein. In diesem Prozess stellt der Router die IPv4-Zieladresse des eingekapselten Headers auf die Routeradresse von Standort B ein. Bei jedem IPv6-Paket, das durch die Tunnelschnittstelle fließt, enthält die IPv6-Zieladresse des Pakets auch die IPv4-Zieladresse. Daher kann der Router die IPv4-Zieladresse feststellen, die im einkapselnden Header eingestellt ist. Dann verwendet der Router standardmäßige IPv4-Routing-Verfahren, um das Paket über das IPv4-Netzwerk weiterzuleiten.
3. Alle IPv4-Router, die die Pakete durchlaufen, verwenden die IPv4-Zieladresse des Pakets zur Weiterleitung. Diese Adresse ist die global einmalige IPv4-Adresse der Schnittstelle auf Router B, die auch als 6to4-Pseudoschnittstelle dient.
4. Pakete von Standort A treffen bei Router B ein, der die IPv6-Pakete aus den IPv4-Headern entkapselt.
5. Router B verwendet dann die Zieladresse im IPv6-Paket, um die Pakete an den Empfangshost an Standort B weiterzuleiten.

Sicherheitsbetrachtungen bei Tunneln zu einem 6to4-Relay-Router

6to4-Relay-Router fungieren als Tunnelendpunkte von 6to4-Routern, die mit nativen IPv6-, nicht-6to4-Netzwerken kommunizieren müssen. Relay-Router sind im Wesentlichen Brücken zwischen einem 6to4-Standort und nativen IPv6-Standorten. Da diese Lösung extrem unsicher ist, aktiviert Oracle Solaris standardmäßig keine Unterstützung für 6to4-Relay-Router. Falls für Ihren Standort ein solcher Tunnel erforderlich ist, können Sie den Befehl `6to4relay` verwenden, um das folgende Tunneling-Szenario zu verwirklichen.

ABBILDUNG 11–7 Tunnel von einem 6to4-Standort zu einem 6to4-Relay-Router



In Abbildung 11–7 muss der 6to4-Standort A mit einem Knoten am nativen IPv6-Standort B kommunizieren. Die Abbildung zeigt den Pfad des Datenverkehrs von Standort A über einen 6to4-Tunnel durch ein IPv4-Netzwerk. Der Tunnel hat den 6to4-Router A und einen 6to4-Relay-Router als Endpunkte. Hinter dem 6to4-Relay-Router befindet sich das IPv6-Netzwerk, mit dem IPv6-Standort B verbunden ist.

Paketfluss zwischen einem 6to4-Standort und einem nativen IPv6-Standort

In diesem Abschnitt wird der Paketfluss von einem 6to4-Standort zu einem nativen IPv6-Standort beschrieben. Das Szenario verwendet die in Abbildung 11–7 gezeigte Topologie.

1. Der Host am 6to4-Standort A sendet eine Übertragung, die einen Host am nativen IPv6-Standort B als Ziel angibt. Jeder Paket-Header weist eine 6to4-abgeleitete Adresse als Quelladresse auf. Die Zieladresse ist eine standardmäßige IPv6-Adresse.

2. Der 6to4-Router an Standort A kapselt jedes Paket in einen IPv4-Header ein, der die IPv4-Adresse des 6to4-Relay-Routers als Ziel angibt. Der 6to4-Router verwendet standardmäßige IPv4-Routing-Verfahren, um das Paket über das IPv4-Netzwerk weiterzuleiten. Alle IPv4-Router, die die Pakete durchlaufen, leiten die Pakete an den 6to4-Relay-Router weiter.
3. Der nächste Anycast 6to4-Relay-Router zu Standort A empfängt die Pakete für die Anycast-Gruppe `192.88.99.1`.

Hinweis – 6to4-Relay-Router sind Teil der 6to4-Relay-Router Anycast-Gruppe mit der IP-Adresse `192.88.99.1` . Diese Anycast-Adresse ist die Standardadresse für 6to4-Relay-Router. Wenn Sie einen bestimmten 6to4-Relay-Router verwenden müssen, können Sie die Standardeinstellung überschreiben und die IPv4-Adresse des Routers angeben.

---

4. Der Relay-Router entkapselt den IPv4-Header von den 6to4-Paketen und legt dabei die native IPv6-Zieladresse frei.
5. Dann sendet der Relay-Router die IPv6-Pakete (jetzt nur IPv6) an das IPv6 Netzwerk weiter, in dem die Pakete letztlich von einem Router an Standort B empfangen werden. Der Router leitet die Pakete dann an den IPv6-Zielknoten weiter.

IPv6-Erweiterungen zu den Oracle Solaris-Namen-Services

In diesem Abschnitt werden die Änderungen bei Benennungen beschrieben, die durch die Umsetzung von IPv6 eingeführt wurden. Sie können IPv6-Adressen in einem beliebigen Oracle Solaris-Namen-Service speichern: NIS, LDAP, DNS und Dateien. Alternativ können Sie NIS over IPv6 RPC-Transporte verwenden, um NIS-Daten abzurufen.

DNS-Erweiterungen für IPv6

Ein IPv6-spezifischer Ressourcendatensatz, der Ressourcendatensatz AAAA, wurde in der RFC 1886 *DNS Extensions to Support IP Version 6* festgelegt. Dieser AAAA-Datensatz wandelt einen Hostnamen in eine 128-Bit-IPv6-Adresse um. Der PTR-Datensatz wird noch immer für IPv6 verwendet, um IP-Adressen in Hostnamen umzuwandeln. Die 32 vier-Bit-Nibbel der 128-Bit-Adresse werden für eine IPv6-Adresse umgekehrt. Jedes Nibble wird in den entsprechenden hexadezimalen ASCII-Wert umgewandelt. Dann wird `ip6.int` angehängt.

Änderungen an der `nsswitch.conf`-Datei

Für Solaris 10 11/06 und früheren Releases wurde neben der Fähigkeit zum Nachschlagen von IPv6-Adressen über die Datei `/etc/inet/ipnodes` eine IPv6-Unterstützung für die

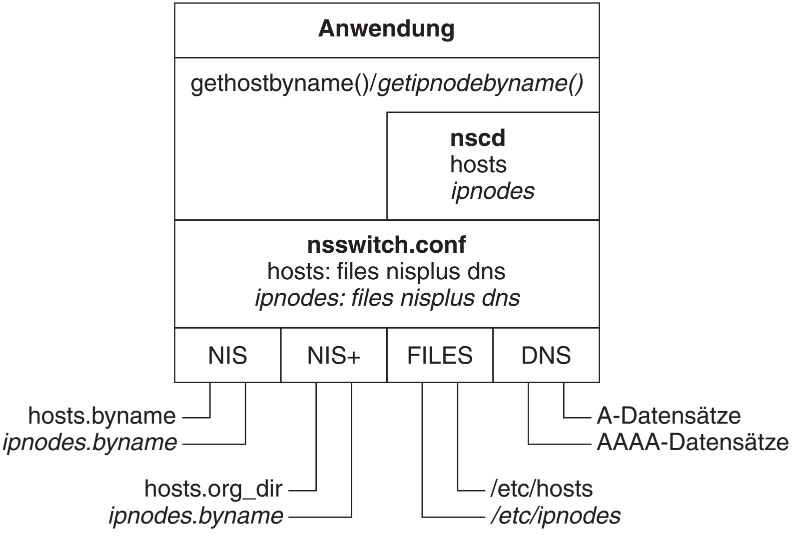
Namen-Services NIS, LDAP und DNS hinzugefügt. Entsprechend wurde die `nsswitch.conf`-Datei modifiziert, um IPv6-Abfragen zu unterstützen.

```
hosts:  files dns nisplus [NOTFOUND=return]
ipnodes: files dns nisplus [NOTFOUND=return]
```

Hinweis – Bevor Änderungen an der `/etc/nsswitch.conf`-Datei vorgenommen werden, um `ipnodes` in mehreren Namen-Services zu durchsuchen, füllen Sie diese `ipnodes`-Datenbanken mit IPv4- und IPv6-Adressen auf. Andernfalls stellen sich unnötige Verzögerungen bei der Auflösung von Hostadressen ein, eventuell sogar Verzögerungen beim Booten.

Das folgende Diagramm zeigt die neue Beziehung zwischen der `nsswitch.conf`-Datei und den neuen Namen-Service-Datenbanken für Anwendungen, die die Befehle `gethostbyname` und `getipnodebyname` verwenden. Kursiv geschriebene Begriffe sind neu. Der Befehl `gethostbyname` prüfte nur, ob IPv4-Adressen in der `/etc/inet/hosts`-Datei gespeichert sind. Unter Solaris 10 11/06 und früheren Releases fragte der Befehl `getipnodebyname` die Datenbank ab, die im Eintrag `ipnodes` in der Datei `nsswitch.conf` angegeben war. Erbrachte diese Suche kein Ergebnis, prüfte der Befehl die Datenbank, die im Eintrag `hosts` in der Dateinsswitch.conf angegeben war.

ABBILDUNG 11–8 Beziehung zwischen der Datei `nsswitch.conf` und Namen-Services



Weitere Informationen zu Namen-Services finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

Änderungen an den Namen-Service-Befehlen

Zur Unterstützung von IPv6 können Sie IPv6-Adressen mit vorhandenen Namen-Service-Befehlen nachschlagen. Beispielsweise arbeitet der Befehl `ypmatch` mit den neuen NIS-Maps. Der Befehl `nslookup` kann die neuen AAAA-Datensätze im DNS nachschlagen.

NFS und RPC IPv6-Unterstützung

NFS-Software und die Remote Procedure Call (RPC)-Software unterstützen IPv6 nahtlos. Vorhandene Befehle für die NFS-Services wurden nicht geändert. Die meisten RPC-Anwendungen führen IPv6 ebenfalls ohne Änderungen aus. Für einige neuere RPC-Anwendungen mit Transportkenntnissen sind eventuell Aktualisierungen erforderlich.

Unterstützung für IPv6-über-ATM

Oracle Solaris unterstützt IPv6-über-ATM, Permanent Virtual Circuits (PVC) sowie statische Switched Virtual Circuits (SVC).

T E I L I I I

DHCP

Dieser Teil enthält konzeptuelle Informationen zum Dynamic Host Configuration Protocol (DHCP) sowie Aufgaben zur Planung, Konfiguration, Verwaltung und Fehlerbehebung des Oracle Solaris DHCP-Service.

KAPITEL 12

Einführung in Oracle Solaris DHCP

Dieses Kapitel enthält eine Einführung in das Dynamic Host Configuration Protocol (DHCP) und beschreibt die diesem Protokoll zu Grunde liegenden Konzepte. Darüber hinaus werden in diesem Kapitel die Vorteile der Verwendung von DHCP in Ihrem Netzwerk beschrieben.

Dieses Kapitel enthält die folgenden Informationen:

- „Einführung in das DHCP-Protokoll“ auf Seite 321
- „Vorteile der Verwendung von Oracle Solaris DHCP“ auf Seite 322
- „Arbeitsweise des DHCP-Protokolls“ auf Seite 323
- „Oracle Solaris DHCP-Server“ auf Seite 326
- „Oracle Solaris DHCP-Client“ auf Seite 336

Einführung in das DHCP-Protokoll

Mit dem DHCP-Protokoll können Hostsysteme in einem TCP/IP-Netzwerk beim Booten automatisch für das Netzwerk konfiguriert werden. DHCP verwendet einen Client-Server-Mechanismus. Server speichern und verwalten Konfigurationsinformationen für Clients und stellen diese Informationen einem Client auf Anforderung zur Verfügung. Zu diesen Informationen zählen die IP-Adresse des Clients sowie Daten zu den Netzwerkservices, die dem Client zur Verfügung gestellt werden.

DHCP hat sich aus einem älteren Protokoll, dem BOOTP-Protokoll entwickelt, das zum Booten über ein TCP/IP-Netzwerk entwickelt wurde. DHCP verwendet das gleiche Format wie BOOTP für Nachrichten zwischen Client und Server. Im Gegensatz zu BOOTP-Nachrichten können DHCP-Nachrichten jedoch Netzwerkkonfigurationsdaten für den Client enthalten.

Ein wesentlicher Vorteil von DHCP ist dessen Fähigkeit, IP-Adresszuweisungen über so genannte „Leasings“ zu verwalten. Mit *Leasings* können IP-Adressen zurückgefordert werden, wenn sie nicht mehr verwendet werden. Die zurückgeforderten IP-Adressen können dann anderen Clients neu zugewiesen werden. Ein Standort, an dem DHCP verwendet wird, kann

einen Pool mit IP-Adressen verwenden, der kleiner ist als eine Konfiguration, bei der allen Clients eine permanente IP-Adresse zugewiesen wird.

Vorteile der Verwendung von Oracle Solaris DHCP

DHCP befreit Sie von einigen zeitintensiven Aufgaben beim Einrichten eines TCP/IP-Netzwerks und der täglichen Verwaltung dieses Netzwerks. Beachten Sie, dass Oracle Solaris DHCP nur mit IPv4 arbeitet.

Oracle Solaris DHCP bietet die folgenden Vorteile:

- **IP-Adressverwaltung** – Ein wesentlicher Vorteil von DHCP ist die einfachere Verwaltung von IP-Adressen. In einem Netzwerk ohne DHCP müssen Sie IP-Adressen manuell zuweisen. Dabei müssen jedem Client einmalige IP-Adressen zugewiesen und jeder Client individuell konfiguriert werden. Falls ein Client in ein anderes Netzwerk verschoben wird, sind manuelle Änderungen an diesem Client erforderlich. Bei aktivierten DHCP verwaltet der DHCP-Server IP-Adressen ohne Administratoreingriff und weist diese zu. Clients können ohne manuelle Neukonfiguration in andere Teilnetze verschoben werden, da sie neue, speziell für das neue Netzwerk passende Clientinformationen vom DHCP-Server beziehen.
- **Zentralisierte Konfiguration von Netzwerkclient** – Sie können eine maßgeschneiderte Konfiguration für bestimmte Clients oder bestimmte Clienttypen erstellen. Die Konfigurationsinformationen werden an einem zentralen Ort, dem DHCP-Datenspeicher abgelegt. Sie müssen sich nicht bei einem Client anmelden, um dessen Konfiguration zu ändern. Änderungen an mehreren Clients werden durchgeführt, indem Sie lediglich die Informationen im Datenspeicher ändern.
- **Unterstützung von BOOTP-Clients** – Sowohl BOOTP-Server als auch DHCP-Server überwachen und reagieren auf Broadcasts von Clients. Der DHCP-Server kann auf Anforderungen von sowohl BOOTP-Clients als auch von DHCP-Clients antworten. BOOTP-Clients erhalten eine IP-Adresse und die zum Booten erforderlichen Informationen von einem Server.
- **Unterstützung von lokalen Clients und remoten Clients** – BOOTP ermöglicht das Weiterschalten von Nachrichten von einem Netzwerk zu einem anderen. DHCP nutzt die Vorteile der BOOTP-Relaisfunktion auf verschiedene Arten. Die meisten Netzwerkrouter können als BOOTP-Relay-Agents konfiguriert werden, um BOOTP-Anforderungen an Server weiterzuleiten, die sich nicht im gleichen Netzwerk wie der Client befinden. DHCP-Anforderungen können auf die gleiche Weise weitergeschaltet werden, da der Router DHCP-Anforderungen nicht von BOOTP-Anforderungen unterscheiden kann. Der Oracle Solaris DHCP-Server kann auch mit dem Verhalten eines BOOTP-Relay-Agent konfiguriert werden, wenn kein Router verfügbar ist, der BOOTP-Relay-Funktionen unterstützt.

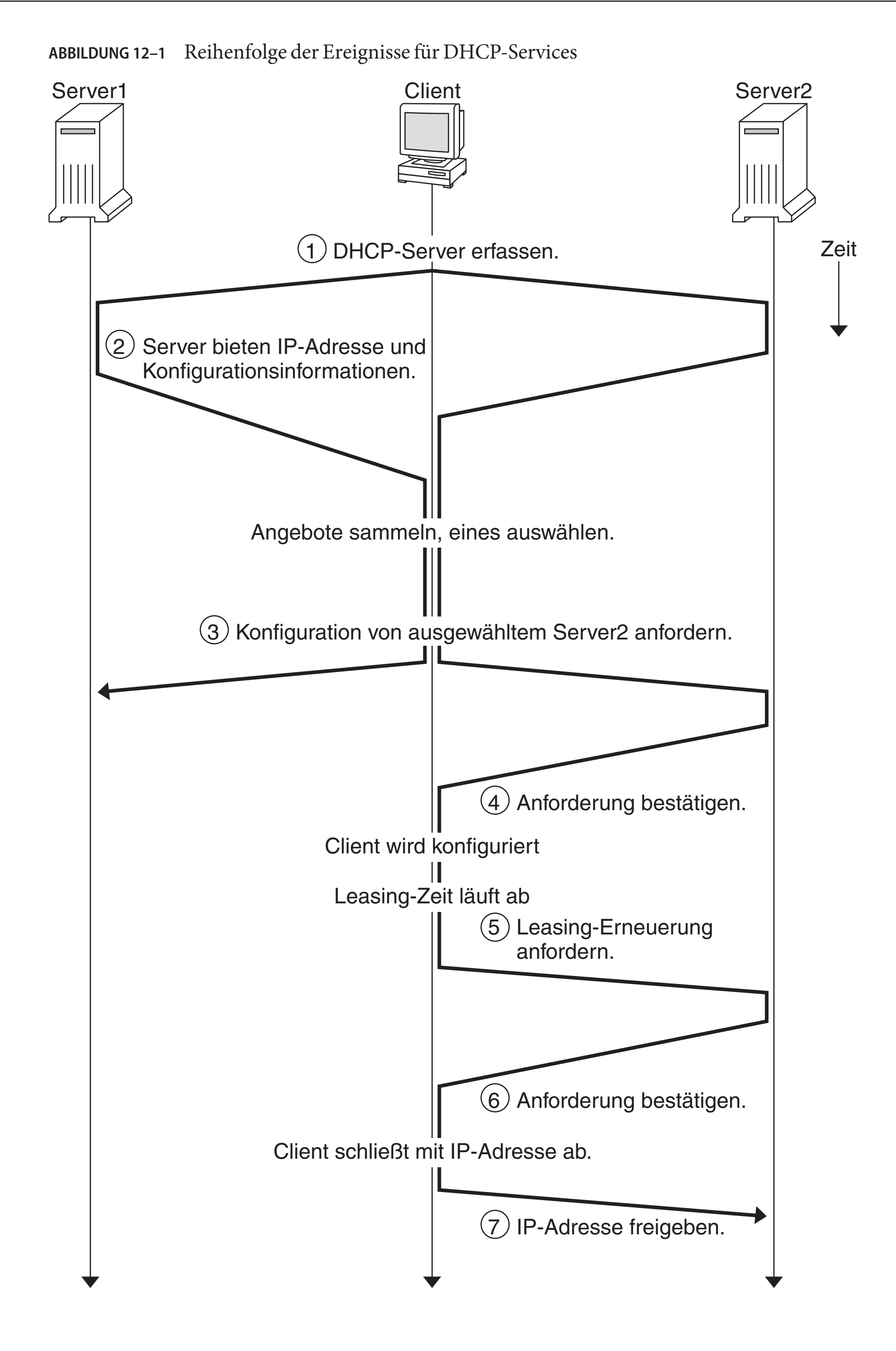
- **Netzwerk-Booten** – Clients können mit DHCP die zum Booten erforderlichen Informationen von einem Server im Netzwerk anstatt über das RARP (Reverse Address Resolution Protocol)-Protokoll und die `bootparams`-Datei beziehen. Der DHCP-Server kann einem Client alle Informationen liefern, die dieser für seine Funktion benötigt, einschließlich IP-Adresse, Boot-Server und Netzwerkkonfigurationsinformationen. Da DHCP-Anforderungen über Teilnetze weitergeschaltet werden können, befinden sind beim DHCP-Netzwerk-Booten weniger Boot-Server im Netzwerk. RARP-Booten erfordert einen Boot-Server in jedem Teilnetz.
- **Unterstützung großer Netzwerke** – Mit Oracle Solaris DHCP können Netzwerke mit Millionen DHCP-Clients verwaltet werden. Der DHCP-Server verwendet Multithreading zur gleichzeitigen Verarbeitung zahlreicher Client-Anforderungen. Darüber hinaus unterstützt der Server Datenspeicher, die zur Verarbeitung großer Datenmengen optimiert wurden. Der Zugriff auf Datenspeicher wird über separate Verarbeitungsmodule abgewickelt. Mit diesem Ansatz können Sie Unterstützung für jede benötigte Datenbank hinzufügen.

Arbeitsweise des DHCP-Protokolls

Zunächst müssen Sie den DHCP-Server installieren und konfigurieren. Während der Konfiguration geben Sie Informationen über das Netzwerk ein, die der Client für die ordnungsgemäße Funktion in diesem Netzwerk benötigt. Nachdem diese Informationen eingerichtet wurden, können Clients Netzwerkinformationen anfordern und empfangen.

Die Reihenfolge der Ereignisse für DHCP-Services wird im folgenden Diagramm gezeigt. Die Zahlen in den Kreisen beziehen sich auf die nummerierten Absätze in der Beschreibung unter dem Diagramm.

ABBILDUNG 12–1 Reihenfolge der Ereignisse für DHCP-Services



Das oben stehende Diagramm zeigt die folgenden Schritte:

1. Der Client erkennt einen DHCP-Server, indem eine *Discovery-Nachricht* an die eingeschränkte Broadcast-Adresse (`255.255.255.255`) im lokalen Teilnetz gesendet wird. Ist ein Router vorhanden, der mit dem Verhalten eines BOOTP-Relay-Agent konfiguriert wurde, wird die Anforderung an weitere DHCP-Server in anderen Teilnetzen weitergeleitet. Die *Broadcast-Nachricht* des Client enthält dessen einmalige ID, die in der DHCP-Implementierung in Oracle Solaris von der Media Access Control (MAC)-Adresse des Clients abgeleitet wurde. In einem Ethernet-Netzwerk gleicht die MAC-Adresse der Ethernet-Adresse.

   DHCP-Server, die diese Discovery-Nachricht empfangen, können das Client-Netzwerk anhand der folgenden Informationen feststellen:

   - Von welcher Netzwerkschnittstelle ist die Anforderung eingegangen? Der Server stellt fest, ob sich der Client in dem Netzwerk befindet, an das die Schnittstelle angeschlossen ist, oder ob der Client einen BOOTP-Relay-Agent verwendet, der an dieses Netzwerk angeschlossen ist.
   - Enthält die Anforderung die IP-Adresse eines BOOTP-Relay-Agent? Wenn die Anforderung über einen Relay-Agent eingegangen ist, fügt der Relay-Agent seine Adresse in den Header der Anforderung ein. Erkennt der Server eine *Relay-Agentadresse*, weiß er, dass die Netzwerkkomponenten der Adresse die Netzwerkadresse des Clients angibt, da der Relay-Agent mit dem Client-Netzwerk verbunden sein muss.
   - Ist das Client-Netzwerk in Teilnetze unterteilt? Der Server durchsucht die `netmasks`-Tabelle nach der Teilnetzmaske des Netzwerks, das durch die Relay-Agentadresse oder durch die Adresse der Netzwerkschnittstelle angegeben wird, die die Anforderung empfangen hat. Sobald der Server die verwendete Teilnetzmaske kennt, kann er feststellen, welcher Teil der Netzwerkadresse die Hostkomponente ist, und kann dann eine für den Client geeignete IP-Adresse auswählen. Weitere Informationen zu `netmasks(4)` finden Sie in der Manpage `netmasks`.
2. Nachdem die DHCP-Server das Client-Netzwerk ermittelt haben, wählen die Server eine geeignete IP-Adresse aus und prüfen, ob diese Adresse bereits verwendet wird. Dann antworten die DHCP-Server dem Client, indem sie eine *Offer-Nachricht* senden. Diese Offer-Nachricht enthält die ausgewählte IP-Adresse und Informationen zu Services, die für den Client konfiguriert werden können. Jeder Server reserviert die angebotene IP-Adresse vorübergehend, bis der Client festlegt, ob diese IP-Adresse verwendet wird.
3. Der Client wählt basierend auf Anzahl und Art der angebotenen Services das beste Angebot aus. Dann sendet der Client eine Anforderung, in der die IP-Adresse des Servers angegeben ist, der das beste Angebot abgegeben hat. Diese Broadcast-Nachricht stellt sicher, dass alle reagierenden DHCP-Server wissen, dass sich der Client für einen Server entschieden hat. Die nicht gewählten Server heben die Reservierungen der angebotenen IP-Adressen auf.

4. Der ausgewählte Server weist dem Client die IP-Adresse zu und speichert die Informationen im DHCP-Datenspeicher. Anschließend sendet der Server eine Bestätigungsnachricht (ACK) an den Client. Diese *Bestätigungsnachricht* enthält die Netzwerkkonfigurationsparameter für den Client. Der Client testet die IP-Adresse mit dem Dienstprogramm `ping`, um sicherzustellen, dass sie von keinem anderen System verwendet wird. Dann setzt der Client das Booten fort, um dem Netzwerk beizutreten.
5. Die Leasing-Zeit wird vom Client überwacht. Wenn der vorgegebene Zeitraum abgelaufen ist, sendet der Client erneut eine Nachricht an den ausgewählten Server, um die Leasing-Zeit zu verlängern.
6. Der DHCP-Server, der diese Anforderung empfängt, verlängert die Leasing-Zeit, wenn das Leasing noch immer der vom Administrator eingerichteten lokalen Leasing-Richtlinie entspricht. Reagiert der Server nicht innerhalb von 20 Sekunden, sendet der Client eine neue Anforderung, so dass einer der anderen DHCP-Server die Leasing-Zeit verlängern kann.
7. Wenn ein Client die IP-Adresse nicht mehr benötigt, informiert er den Server, dass die IP-Adresse freigegeben wurde. Diese Benachrichtigung kann während des ordnungsgemäßen Herunterfahrens oder auch manuell erfolgen.

Oracle Solaris DHCP-Server

Der Oracle Solaris DHCP-Server wird als ein Daemon in Oracle Solaris auf einem Hostsystem ausgeführt. Der Server hat zwei allgemeine Funktionen:

- **Verwalten von IP-Adressen** – Der DHCP-Server kontrolliert einen Bereich von IP-Adressen und weist sie Clients entweder permanent oder für einen festgelegten Zeitraum zu. Der Server nutzt einen Leasing-Mechanismus, um festzustellen, wie lange ein Client eine nicht-permanente Adresse verwenden kann. Wird eine Adresse nicht mehr benötigt, kehrt sie in den Pool zurück und kann neu zugewiesen werden. Der Server verwaltet die Informationen zur Bindung von IP-Adressen an Clients in DHCP-Netzwerktabellen und stellt so sicher, dass keine Adresse von mehreren Clients genutzt wird.
- **Bereitstellen der Netzwerkkonfiguration für Clients** – Der Server weist eine IP-Adresse zu und stellt weitere Informationen zur Netzwerkkonfiguration bereit. Hierzu gehören z. B. Hostname, Broadcast-Adresse, Netzwerk-Teilnetzmaske, Standard-Gateway, Namen-Service und weitere Informationen. Die Netzwerkkonfigurationsinformationen werden aus der `dhcptab`-Datenbank des Servers bezogen.

Der Oracle Solaris DHCP-Server kann auch zur Ausführung der folgenden zusätzlichen Funktionen konfiguriert werden:

- **Beantworten von BOOTP-Client-Anforderungen** – Der Server überwacht auf Broadcasts von BOOTP-Clients zum Erfassen eines BOOTP-Servers und stellt ihnen eine IP-Adresse und Boot-Parameter zur Verfügung. Die Informationen müssen von einem Administrator statisch konfiguriert worden sein. Der DHCP-Server kann gleichzeitig als BOOTP-Server und als DHCP-Server fungieren.
- **Weiterschalten von Anforderungen** – Der Server schaltet BOOTP- und DHCP-Anforderungen an die entsprechenden Server in anderen Teilnetzen weiter. Wenn der Server als BOOTP-Relay-Agent konfiguriert ist, kann er keine DHCP- oder BOOTP-Services bereitstellen.
- **Bereitstellen der Netzwerk-Boot-Unterstützung für DHCP-Clients** – Der Server kann DHCP-Clients Informationen bereitstellen, die zum Booten über das Netzwerk erforderlich sind: eine IP-Adresse, Boot-Parameter sowie Netzwerkkonfigurationsinformationen. Darüber hinaus kann der Server Informationen bereitstellen, die DHCP-Clients zum Booten und zur Installation über ein WAN benötigen.
- **Aktualisieren der DNS-Tabellen für Clients, die einen Hostnamen angeben** – Für Clients, die eine `Hostname`-Option und einen Wert in ihren Anforderungen nach einem DHCP-Service angeben, kann der Server DNS-Aktualisierungen in deren Auftrag versuchen.

Verwaltung eines DHCP-Servers

Als Superuser können Sie den DHCP-Server mit DHCP Manager oder einem der unter „DHCP-Befehlszeilenprogramme" auf Seite 330 beschriebenen Befehlszeilenprogramme starten, stoppen und konfigurieren. Im Allgemeinen ist der DHCP-Server so konfiguriert, dass er automatisch beim Booten des Systems gestartet und beim Herunterfahren des Systems gestoppt wird. Unter normalen Bedingungen müssen Sie dem Server weder manuell starten noch stoppen.

DHCP-Datenspeicher

Alle vom Oracle Solaris DHCP-Server verwendeten Daten werden in einem Datenspeicher verwaltet. Der Datenspeicher enthält reine Textdateien, NIS+-Tabellen oder Dateien im Binärformat. Bei der Konfiguration des DHCP-Service legen Sie den zu verwendenden Datenspeichertyp fest. Die Unterschiede zwischen den Datenspeichertypen werden im Abschnitt „Auswählen des DHCP-Datenspeichers" auf Seite 343 beschrieben. Der Datenspeicher kann mithilfe von DHCP Manager oder dem Befehl `dhcpconfig` in einen anderen Formattyp umgewandelt werden.

Sie können die Daten auch aus dem Datenspeicher eines DHCP-Servers in den Datenspeicher eines anderen Servers verschieben. Zum Exportieren und Importieren von Datenspeicherinhalten stehen Ihnen verschiedene Dienstprogramme zur Verfügung, mit denen Sie auch dann arbeiten können, wenn die Server Daten in unterschiedlichen Formaten speichern. Mit DHCP Manager oder dem Befehl `dhcpconfig` können Sie entweder den gesamten Inhalt eines Datenspeichers importieren oder exportieren, oder nur einige der darin enthaltenen Daten.

Hinweis – Sie können jedes Datenbank- oder Dateiformat für einen DHCP-Datenspeicher verwenden, vorausgesetzt, Sie entwickeln Ihr eigenes Codemodul, um eine Schnittstelle zwischen Oracle Solaris DHCP (Server- und Verwaltungstools) und der Datenbank zu schaffen. Weitere Informationen finden Sie im *Solaris DHCP Service Developer's Guide* .

Im Oracle Solaris DHCP-Datenspeicher gibt es zwei Arten von Tabellen. Sie können die Inhalte dieser Tabellen entweder mit DHCP Manager oder den Befehlszeilenprogrammen anzeigen und verwalten. Die Datentabellen sind:

- `dhcptab`-**Tabelle** – Eine Tabelle mit den Konfigurationsinformationen, die an Clients weitergegeben werden.
- **DHCP-Netzwerktabellen** – Diese Tabellen enthalten Informationen zu den DHCP- und BOOTP-Clients, die sich in dem Netzwerk befinden, das im Tabellennamen angegeben ist. Beispielsweise hat das Netzwerk `192.168.32.0` eine Tabelle mit dem Namen `192_168_32_0`.

Die `dhcptab`-Tabelle

Die `dhcptab`-Tabelle enthält alle Informationen, die Clients vom DHCP-Server beziehen können. Der DHCP-Server scannt die `dhcptab`-Tabelle bei jedem Start. Der Dateiname der `dhcptab`-Tabelle hängt von dem verwendeten Datenspeichertyp ab. So lautet der Name der `dhcptab`-Tabelle, die von dem NIS+-Datenspeicher `SUNWnisplus` erstellt wurde, `SUNWnisplus1_dhcptab`.

Das DHCP-Protokoll definiert zahlreiche Standardinformationen, die an Clients weitergegeben werden können. Diese Informationen werden als Parameter, Symbole oder Optionen bezeichnet. Optionen sind im DHCP-Protokoll durch numerische Codes und Textbezeichnungen definiert, enthalten aber keine Werte. Einige häufig verwendete Standardoptionen sind in der folgenden Tabelle aufgeführt.

TABELLE 12–1 Beispiele für DHCP-Standardoptionen

Code	Bezeichnung	Beschreibung
1	`Subnet`	IP-Adresse der Teilnetzmaske
3	`Router`	IP-Adresse des Routers

TABELLE 12–1 Beispiele für DHCP-Standardoptionen (Fortsetzung)

Code	Bezeichnung	Beschreibung
6	DNSserv	IP-Adresse des DNS-Servers
12	Hostname	Textstring für den Client-Hostnamen
15	DNSdmain	DNS-Domänenname

Einige Optionen werden den Werten automatisch zugewiesen, wenn Sie schon bei der Serverkonfiguration Daten angeben. Sie können auch zu einem späteren Zeitpunkt explizite Werte zuweisen. Optionen und deren Werte werden an den Client übergeben, um Konfigurationsinformationen bereitzustellen. Beispielsweise setzt das Option/Wert-Paar `DNSdmain=Georgia.Peach.COM` den DNS-Domänennamen des Clients auf `Georgia.Peach.COM`.

Optionen können in Containern gruppiert werden, die als *Makros* bezeichnet werden und die Übergabe von Informationen an einen Client vereinfachen. Einige Makros werden während der Serverkonfiguration automatisch erstellt und enthalten Optionen, denen während der Konfiguration Werte zugewiesen werden. Makros können auch weitere Makros enthalten.

Das Format der `dhcptab`-Tabelle ist in der Manpage `dhcptab(4)` beschrieben. In DHCP Manager stammen alle Informationen, die auf den Registerkarten „Optionen“ und „Makros“ angezeigt werden, aus der `dhcptab`-Tabelle. Weitere Informationen zu Optionen finden Sie unter „Einführung in DHCP-Optionen“ auf Seite 333 Weitere Informationen zu Makros finden Sie unter „Einführung in DHCP-Makros“ auf Seite 334.

Die `dhcptab`-Tabelle sollte nicht manuell bearbeitet werden. Verwenden Sie zum Erstellen, Löschen oder Bearbeiten von Optionen und Makros entweder den Befehl `dhtadm` oder DHCP Manager.

DHCP-Netzwerktabellen

Eine DHCP-Netzwerktabelle weist Client-Bezeichnungen korrekte IP-Adressen und Konfigurationsparameter zu, die jeder Adresse zugeordnet sind. Das Format der Netzwerktabellen ist in der Manpage `dhcp_network(4)` beschrieben. In DHCP Manager stammen alle Informationen, die auf der Registerkarte „Adressen“ angezeigt werden, aus den Netzwerktabellen.

DHCP Manager

DHCP Manager ist ein Tool mit grafischen Benutzeroberfläche (GUI), mit dem Sie alle Verwaltungsaufgaben durchführen können, die dem DHCP-Service zugeordnet sind. Mit diesem Tool können Sie den Server sowie alle Daten verwalten, die der Server verwendet. Zum Ausführen von DHCP Manager müssen Sie als Superuser angemeldet sein.

Sie können DHCP Manager mit dem Server für Folgendes verwenden:

- Konfigurieren und Dekonfigurieren eines DHCP-Servers
- Starten, Stoppen und Neustarten des DHCP-Servers
- Deaktivieren und Aktivieren des DHCP-Services
- Anpassen der DHCP-Servereinstellungen

Mit DHCP Manager können Sie die IP-Adressen, Netzwerkkonfigurationsmakros und Netzwerkkonfigurationsoptionen auf folgende Arten verwalten:

- Hinzufügen und Löschen von Netzwerken unter der DHCP-Verwaltung
- Anzeigen, Hinzufügen, Modifizieren, Löschen und Freigeben von IP-Adressen unter der DHCP-Verwaltung
- Anzeigen, Hinzufügen, Modifizieren und Löschen von Netzwerkkonfigurationsmakros
- Anzeigen, Hinzufügen, Modifizieren und Löschen von nicht dem Standard entsprechenden Netzwerkkonfigurationsoptionen

Mit DHCP Manager können Sie folgende Aktionen an DHCP-Datenspeichern durchführen:

- Konvertieren von Daten in ein neues Datenspeicherformat
- Verschieben von DHCP-Daten von einem DHCP-Server auf einen anderen, in dem Sie die Daten auf dem ersten Server exportieren und auf dem zweiten Server importieren

DHCP Manager umfasst eine umfangreiche Onlinehilfe, in der die Verfahren beschrieben werden, die Sie mit dem Tool durchführen können. Weitere Informationen finden Sie unter „Allgemeines zum DHCP Manager" auf Seite 368.

DHCP-Befehlszeilenprogramme

Alle DHCP-Verwaltungsfunktionen können auch mithilfe von Befehlszeilenprogrammen aufgerufen werden. Sie können diese Dienstprogramme nur dann ausführen, wenn Sie als Superuser angemeldet oder Ihnen das DHCP Management-Profil zugewiesen wurde. Lesen Sie dazu „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

In der folgenden Tabelle sind die Dienstprogramme und die Aufgaben jedes Dienstprogramms aufgeführt.

TABELLE 12–2 DHCP-Befehlszeilenprogramme

Befehl	Beschreibung und Zweck	Manpage-Links
`in.dhcpd`	Der DHCP-Servicedaemon. Mit Befehlszeilenargumenten können Sie verschiedene Laufzeitoptionen einstellen.	`in.dhcpd(1M)`

TABELLE 12–2 DHCP-Befehlszeilenprogramme *(Fortsetzung)*

Befehl	Beschreibung und Zweck	Manpage-Links
`dhcpconfig`	Dient zur Konfiguration und Dekonfiguration eines DHCP-Servers. Mit diesem Dienstprogramm können Sie viele der Funktionen von DHCP Manager von einer Befehlszeile aus aufrufen. Dieses Dienstprogramm wird im Wesentlichen in Skripten für Standorte verwendet, mit denen bestimmte Konfigurationsfunktionen automatisiert werden sollen. `dhcpconfig` sammelt Informationen von den Netzwerk-Topologiedateien des Serversystems, um nützliche Informationen zur Erstkonfiguration zu erzeugen.	`dhcpconfig`(1M)
`dhtadm`	Dient zum Hinzufügen, Löschen und Modifizieren von Konfigurationsoptionen und -makros für DHCP-Clients. Mit diesem Dienstprogramm können Sie die `dhcptab`-Tabelle indirekt bearbeiten. So wird sichergestellt, dass für die `dhcptab`-Tabelle das korrekte Format verwendet wird. Sie sollten die `dhcptab`-Tabelle nicht direkt bearbeiten.	`dhtadm`(1M)
`pntadm`	Dient zum Verwalten der DHCP-Netzwerktabellen. Mit diesem Dienstprogramm können Sie die folgenden Aufgaben ausführen: ■ Hinzufügen und Entfernen von IP-Adressen und Netzwerken unter der DHCP-Verwaltung. ■ Modifizieren der Netzwerkkonfiguration für bestimmte IP-Adressen. ■ Anzeigen von Informationen zu IP-Adressen und Netzwerken unter der DHCP-Verwaltung.	`pntadm`(1M)

Rollenbasierte Zugriffskontrolle für DHCP-Befehle

Die Sicherheit für die Befehle `dhcpconfig`, `dhtadm` und `pntadm` wird über die Einstellungen der rollenbasierten Zugriffskontrolle (Role-Based Access Control, RBAC) eingerichtet. Standardmäßig können die Befehle nur von einem Superuser ausgeführt werden. Wenn Sie die Befehle unter einem anderen Benutzernamen ausführen möchten, müssen Sie diesem Benutzernamen das DHCP Management-Profil zuweisen. Eine Beschreibung hierzu finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

Konfiguration eines DHCP-Servers

Sie konfigurieren den Oracle Solaris DHCP-Server, wenn Sie DHCP Manager das erste Mal auf dem System starten, auf dem der DHCP-Server ausgeführt werden soll.

In den Dialogfeldern zur Serverkonfiguration in DHCP Manager werden Sie zur Eingabe von Daten aufgefordert, die zum Aktivieren und Ausführen des DHCP-Servers in einem Netzwerk erforderlich sind. Einige Standardwerte werden aus bereits vorhandenen Systemdateien bezogen. Wenn Sie das System nicht für das Netzwerk konfiguriert haben, stehen keine Standardwerte zur Verfügung. DHCP Manager fordert Sie zur Eingabe der folgenden Informationen auf:

- Rolle des Servers, entweder DHCP-Server oder BOOTP-Relay-Agent
- Datenspeichertyp (Dateien, Binärdateien, NIS+ oder ein Standort-spezifisches Format)
- Datenspeicher-Konfigurationsparametern für den von Ihnen ausgewählten Datenspeichertyp
- Zum Aktualisieren der Hostdatensätze zu verwendender Namen-Service, sofern erforderlich (`/etc/hosts` , NIS+ oder DNS)
- Dauer der Leasing-Zeit und ob Clients in der Lage sein sollen, Leasings zu erneuern
- DNS-Domänennamen und IP-Adressen der DNS-Server
- Netzwerkadresse und Teilnetzmaske des ersten Netzwerks, das Sie für den DHCP-Service konfigurierenden möchten
- Netzwerktyp, entweder LAN oder Point-to-Point-Netzwerk
- Router-Erkennung oder IP-Adressen eines bestimmten Routers
- NIS-Domänennamen und IP-Adressen der NIS-Server
- NIS+-Domänenname und IP-Adressen der NIS+-Server

Sie können den DHCP-Server auch mithilfe des Befehls `dhcpconfig` konfigurieren. Dieses Dienstprogramm sammelt automatisch Informationen aus vorhandenen Systemdateien, und stellt nützliche Informationen zur Erstkonfiguration zusammen. Aus diesem Grund müssen Sie vor dem Ausführen von `dhcpconfig` sicherstellen, dass die Dateien korrekt sind. Informationen zu Dateien, die den Befehl `dhcpconfig` zum Beziehen von Informationen verwenden, finden Sie in der Manpage `dhcpconfig(1M)`.

Zuweisung von IP-Adressen

Der Oracle Solaris DHCP-Server unterstützt die folgenden Arten der Zuweisung von IP-Adressen:

- **Manuelle Zuweisung** – Der Server stellt eine bestimmte IP-Adresse zur Verfügung, die Sie für einen bestimmten DHCP-Client wählen können. Die Adresse kann nicht zurückgefordert oder einem anderen Client zugewiesen werden.
- **Automatische oder permanente Zuweisung** – Der Server stellt eine IP-Adresse ohne Ablaufdatum zur Verfügung, die dem Client permanent zugewiesen wird, bis Sie die Zuweisung aufheben oder der Client die Adresse freigibt.
- **Dynamische Zuweisung** – Der Server stellt dem anfordernden Client eine IP-Adresse als Leasing für einen bestimmten Zeitraum zur Verfügung. Wenn das Leasing abgelaufen ist, wird die Adresse vom Server zurückgenommen und kann einem anderen Client zugewiesen werden. Die Leasing-Dauer wird durch die für den Server konfigurierte Leasing-Zeit festgelegt.

Netzwerkkonfigurationsinformationen

Sie können festlegen, welche Informationen DHCP-Clients bereitgestellt werden sollen. Wenn Sie den DHCP-Server konfigurieren, stellen Sie die wichtigsten Informationen zum Netzwerk zur Verfügung. Später können Sie weitere Informationen hinzufügen, die den Clients bereitgestellt werden sollen.

Der DHCP-Server speichert Netzwerkkonfigurationsinformationen in Form von Option/Wert-Paaren und Makros in der `dhcptab` -Tabelle. Optionen sind Schlüsselwörter für Netzwerkdaten, die Sie Clients bereitstellen möchten. Den Optionen sind Werte zugewiesen, die in DHCP-Nachrichten an die Clients übergeben werden. Beispielsweise wird die NIS mit einer Option namens `NISservs` übergeben. Die `NISservs`-Option verfügt über einen Wert, der einer Liste mit IP-Adressen gleicht, die vom DHCP-Server zugewiesen wurde. Mit Makros können Sie eine beliebige Anzahl Optionen gruppieren, die Clients bereitgestellt werden sollen. Mit DHCP Manager können Sie Makros erstellen, um Optionen zu gruppieren und ihnen Werte zuzuweisen. Wenn Sie ein Befehlszeilenprogramm bevorzugen, können Sie `dhtadm`, das Verwaltungsprogramm für DHCP-Konfigurationstabellen verwenden, um mit Optionen und Makros zu arbeiten.

Einführung in DHCP-Optionen

Unter Oracle Solaris DHCP stellt eine *Option* einen Satz mit Netzwerkinformationen dar, die an einem Client übergeben werden. Die DHCP-Literatur bezeichnet Optionen auch als *Symbole* oder *Tags*. Eine Option wird durch einen numerischen Code und eine Textbezeichnung definiert. Eine Option erhält einen Wert, wenn sie im DHCP-Service verwendet wird.

Das DHCP-Protokoll definiert zahlreiche Standardoptionen für häufig angegebene Netzwerkdaten: `Subnet`, `Router`, `Broadcst`, `NIS+dom`, `Hostname` und `LeaseTim` sind einige Beispiele dafür. Eine vollständige Liste der Standardoptionen finden Sie in der Manpage `dhcp_inittab(4)` Die Schlüsselwörter von Standardoptionen können nicht geändert werden. Sie können den Optionen jedoch Werte zuweisen, die für Ihr Netzwerk relevant sind, wenn Sie die Optionen in Makros aufnehmen.

Sie können auch neue Optionen für Daten erstellen, für die keine Standardoptionen vorhanden sind. Von Ihnen erstellte Optionen müssen in eine der folgenden drei Kategorien fallen:

- **Erweitert** – Reserviert für Optionen, die standardmäßige DHCP-Optionen geworden sind, aber noch nicht in der Implementierung des DHCP-Servers enthalten sind. Sie können eine erweiterte Option verwenden, wenn Sie eine mögliche Standardoption kennen, aber Ihren DHCP-Server nicht aktualisieren möchten.
- **Standort** – Reserviert für Optionen, die einmalig für Ihren Standort sind. Diese Optionen werden von Ihnen erstellt.
- **Hersteller** – Reserviert für Optionen, die nur für Clients einer bestimmten Klasse gelten, z. B. eine bestimmte Hardware- oder Anbieterplattform. Die Oracle Solaris DHCP-Implementierung umfasst zahlreiche Hersteller-Optionen für Oracle Solaris-Clients. Beispielsweise wird die Option `SrootIP4` dazu verwendet, die IP-Adressen eines Servers anzugeben, die ein Client, der über das Netzwerk bootet, als Root-Dateisystem (/) verwenden soll.

Kapitel 15, „Verwalten von DHCP (Aufgaben)“ enthält Verfahren zum Erstellen, Bearbeiten und Löschen von DHCP-Optionen.

Einführung in DHCP-Makros

In der Oracle Solaris DHCP-Service-Terminologie ist ein *Makro* eine Sammlung von Netzwerkkonfigurationsoptionen und den Werten, die Sie diesen Optionen zuweisen. Makros dienen zum Gruppieren von Optionen, die an bestimmte Clients oder Clienttypen übergeben werden. Beispielsweise könnte ein Makro, das an alle Clients eines bestimmten Teilnetzes übergeben werden soll, Option/Wert-Paare für Teilnetzmaske, Router-IP-Adressen, Broadcast-Adresse, NIS+-Domäne und Leasing-Zeit enthalten.

Von DHCP-Server verarbeitete Makros

Wenn ein DHCP-Server ein Makro verarbeitet, platziert er die Netzwerkoptionen und Werte, die in dem Makro definiert sind, in einer DHCP-Nachricht an den Client. Bestimmte Makros für Clients eines bestimmten Typs verarbeitet der Server automatisch.

Damit der Server ein Makro automatisch verarbeiten kann, muss der Name des Makros in eine der in der folgenden Tabelle aufgeführten Kategorien fallen.

TABELLE 12–3 DHCP-Makrokategorien zur automatischen Verarbeitung

Makrokategorie	Beschreibung
Clientklasse	Der Makroname entspricht einer Clientklasse, gekennzeichnet durch den Client-Computertyp, das Betriebssystem oder beidem. Angenommen, der Server hat ein Makro namens `SUNW.Sun-Blade-100`. Alle Clients, deren Hardware-Implementierung `SUNW,Sun-Blade-100` lautet, empfangen automatisch die Werte im Makro `SUNW.Sun-Blade-100`.
Netzwerkadresse	Der Makroname entspricht einer DHCP-verwalteten Netzwerk-IP-Adresse. Angenommen, ein Server hat ein Makro namens `10.53.224.0`. Jeder Client, der mit dem Netzwerk `10.53.224.0` verbunden ist, erhält automatisch die Werte im Makro `10.53.224.0`.
Client-ID	Der Makroname entspricht einem einmaligen Bezeichner für einen Client, der in der Regel von einer Ethernet- oder MAC-Adresse abgeleitet wird. Angenommen, ein Server hat ein Makro namens `08002011DF32`. Der Client mit Client-ID `08002011DF32` (abgeleitet von der Ethernet-Adresse `8:0:20:11:DF:32`) erhält automatisch die Werte in dem Makro mit der Bezeichnung `08002011DF32`.

Ein Makro mit einem Namen, der keine der in Tabelle 12–3 aufgeführten Kategorien entspricht, kann nur dann verarbeitet werden, wenn eine der folgenden Bedingungen zutrifft:

- Das Makro ist einer IP-Adresse zugeordnet.
- Das Makro ist in einem anderen Makro enthalten, das automatisch verarbeitet wird.
- Das Makro ist in einem anderen Makro enthalten, das einer IP-Adresse zugeordnet ist.

Hinweis – Wenn Sie einem Server konfigurieren, wird standardmäßig ein Makro erstellt, dessen Name dem Servernamen entspricht. Das Servermakro wird *nicht* automatisch für Clients verarbeitet, da es nicht mit einem der Namenstypen bezeichnet ist, der eine automatische Verarbeitung auslöst. Wenn Sie später IP-Adressen auf dem Server erstellen, werden diese so zugeordnet, dass sie standardmäßig das Servermakro verwenden.

Reihenfolge der Makroverarbeitung

Wenn ein DHCP-Client DHCP-Services anfordert, stellt der DHCP-Server fest, welche Makros den Client entsprechen. Der Server verarbeitet die Makros unter Verwendung der Makrokategorien, um die Verarbeitungsreihenfolge festzulegen. Die allgemeine Kategorie wird zuerst verarbeitet, eine spezielle Kategorie zuletzt. Die Makros werden in der folgenden Reihenfolge verarbeitet:

1. Clientklasse-Makros – Die allgemeine Kategorie
2. Netzwerkadresse-Makros – Spezieller als die Clientklasse
3. Makros, die IP-Adressen zugeordnet sind – Spezieller als die Netzwerkadresse
4. Client-ID-Makros – Die speziellste Kategorie, betrifft nur einen Client

Ein Makro, das in einem anderen Makro enthalten ist, wird als Teil des Container-Makros verarbeitet.

Wenn die gleiche Option in mehreren Makros enthalten ist, wird der Wert für diese Option in der speziellsten Kategorie verwendet, da er als letztes verarbeitet wird. Angenommen, ein Netzwerkadresse-Makro enthält die Leasing-Zeit-Option mit einem Wert von 24 Stunden, und ein Client-ID-Makro enthält den Wert 8 Stunden, so erhält der Client eine Leasing-Zeit von 8 Stunden.

Größenbeschränkung für DHCP-Makros

Die Gesamtsumme der Werte, die anderen Optionen in einem Makro zugewiesen wird, darf, einschließlich Optionscodes und Längeninformationen, 255 Byte nicht überschreiten. Diese Grenze wird durch das DHCP-Protokoll vorgeschrieben.

Diese Größenbeschränkung wirkt sich am ehesten auf Makros aus, die zur Übergabe von Pfaden zu Dateien auf Oracle Solaris-Installationsservern verwendet werden. Im Allgemeinen sollten Sie nur die Mindestmenge der erforderlichen Anbieterinformationen übergeben. Sie sollten kurze Pfadnamen für Optionen verwenden, die Pfadnamen verlangen. Wenn Sie symbolische Links zu langen Pfaden erstellen, können Sie die kürzeren Linknamen übergeben.

Oracle Solaris DHCP-Client

Der Begriff „Client“ wird manchmal auch verwendet, um einen realen Computer zu bezeichnen, der eine Clientrolle in einem Netzwerk ausführt. Bei dem in diesem Dokument beschriebenen DHCP-Client handelt es sich jedoch um eine Software-Entität. Der Oracle Solaris DHCP-Client ist ein Daemon (`dhcpagent`), der in Oracle Solaris auf einem System ausgeführt wird, das dazu konfiguriert wurde, die Netzwerkkonfiguration von einem DHCP-Server zu erhalten. DHCP-Clients von anderen Anbietern können die Services des Oracle Solaris-DHCP-Servers ebenfalls nutzen. In diesem Dokument wird jedoch nur der Oracle Solaris DHCP-Client beschrieben.

Ausführliche Informationen zum Oracle Solaris DHCP-Client finden Sie in Kapitel 16, „Konfiguration und Verwaltung des DHCP-Clients“.

KAPITEL 13

Planungen für den DHCP-Service (Aufgaben)

Sie können den DHCP-Service in einem von Ihnen erstellten oder einem bereits vorhandenen Netzwerk verwenden. Wenn Sie ein neues Netzwerk einrichten, lesen Sie Kapitel 2, „Planen Ihres TCP/IP-Netzwerks (Vorgehen)“, bevor Sie versuchen, den DHCP-Service einzurichten. Wenn das Netzwerk bereits besteht, lesen Sie in diesem Kapitel weiter.

In diesem Kapitel wird beschrieben, was Sie ausführen müssen, bevor Sie den DHCP-Service in Ihrem Netzwerk einrichten können. Bei den Informationen wird davon ausgegangen, dass Sie mit DHCP Manager arbeiten, obwohl Sie auch das Befehlszeilenprogramm `dhcpconfig` zum Einrichten des DHCP-Services verwenden können.

Dieses Kapitel enthält die folgenden Informationen:

- „Vorbereiten Ihres Netzwerks für den DHCP-Service (Übersicht der Schritte)“ auf Seite 337
- „Entscheidungen bei der Konfiguration Ihres DHCP-Servers (Übersicht der Schritte)“ auf Seite 342
- „Entscheidungen bei der Verwaltung von IP-Adressen (Übersicht der Schritte)“ auf Seite 346
- „Planung für mehrere DHCP-Server“ auf Seite 350
- „Planung einer DHCP-Konfiguration für remote Netzwerke“ auf Seite 351
- „Auswählen des Tools zur Konfiguration von DHCP“ auf Seite 351

Vorbereiten Ihres Netzwerks für den DHCP-Service (Übersicht der Schritte)

Bevor Sie Ihr Netzwerk zur Verwendung von DHCP einrichten, müssen Sie Informationen zusammenstellen, die Sie bei der Konfiguration eines oder mehrerer Server unterstützen. In der folgenden Übersicht finden Sie die Aufgaben, die zur Vorbereitung Ihres Netzwerks für den DHCP-Service ausgeführt werden müssen. Die Tabelle enthält Aufgaben, Beschreibungen zum Zweck dieser Aufgaben und Abschnitte, in denen die Schritte zur Ausführung der einzelnen Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
Erstellen einer Topologieübersicht Ihres Netzwerks.	Ermitteln und lokalisieren Sie die im Netzwerk zur Verfügung stehenden Services.	„Erstellen einer Netzwerktopologie“ auf Seite 338
Ermitteln der Anzahl der erforderlichen DHCP-Server.	Verwenden Sie die zu erwartende Anzahl der DHCP-Clients als Grundlage, um die Anzahl der erforderlichen DHCP-Server festzulegen.	„Festlegen der Anzahl von DHCP-Servern“ auf Seite 339
Aktualisieren von Systemdateien und der `netmasks`-Tabelle.	Geben Sie die Netzwerktopologie exakt wieder.	„Aktualisieren von Systemdateien und Netzmasken-Tabellen“ auf Seite 340

Erstellen einer Netzwerktopologie

Falls Sie es noch nicht getan haben, erstellen Sie jetzt eine Übersicht der Struktur Ihres Netzwerks. Geben Sie die Positionen von Routern und Clients an, sowie die Positionen von Servern, die Netzwerkservices bereitstellen. Diese Karte Ihrer Netzwerktopologie hilft Ihnen dabei festzustellen, welche Server für DHCP-Services verwendet werden sollen. Darüber hinaus hilft Ihnen die Karte dabei, die Konfigurationsinformationen festzulegen, die der DHCP-Server Clients bereitstellen kann.

Weitere Informationen zur Planung Ihres Netzwerks finden Sie in Kapitel 2, „Planen Ihres TCP/IP-Netzwerks (Vorgehen)“.

Der DHCP-Konfigurationsprozess kann Netzwerkinformationen aus den Systemen- und Netzwerkdateien des Servers beziehen. Diese Dateien werden unter „Aktualisieren von Systemdateien und Netzmasken-Tabellen“ auf Seite 340 beschrieben. Wahrscheinlich möchten Sie den Clients jedoch weitere Informationen zum DHCP-Service bereitstellen, die Sie in die Server-Makros eingeben müssen. Zeichnen Sie beim Zusammenstellen der Netzwerktopologie die IP-Adressen aller Server auf, die den Clients bekannt sein müssen. Beispielsweise können die folgenden Server Services für Ihr Netzwerk bereitstellen. Dieser Server werden von der DHCP-Konfiguration nicht erfasst.

- Zeitserver
- Protokollserver
- Druckserver
- Installationsserver
- Boot-Server
- Web-Proxy-Server
- Swap-Server
- X Window Font-Server
- Trivial File Transfer Protocol (TFTP)-Server

Zu vermeidenden Netzwerktopologie

In einigen IP-Netzwerkumgebungen nutzen mehrere LANs die gleichen Netzwerk-Hardware-Medien gemeinsam. Die Netzwerke können mehrere Netzwerk-Hardwareschnittstellen oder mehrere logische Schnittstellen verwenden. DHCP arbeitet bei diesem Netzwerktyp mit gemeinsam genutzte Medien möglicherweise fehlerhaft. Wenn mehrere LANs über das gleiche physikalische Netzwerk ausgeführt werden, treffen die Anforderungen eines DHCP-Clients an allen Netzwerk-Hardwareschnittstellen ein. Dadurch scheint es, als wäre der Client mit allen IP-Netzwerken gleichzeitig verbunden.

DHCP muss jedoch in der Lage sein, die Adresse des Client-Netzwerks zu ermitteln, um dem Client eine korrekte IP-Adresse zuweisen zu können. Wenn mehrere Netzwerke in den gleichen Hardwaremedien vorhanden sind, kann der Server das Client-Netzwerk nicht feststellen. Jedoch kann der Server keine IP-Adresse zuweisen, ohne die Netzwerknummer zu kennen.

Sie können DHCP nur in einem dieser Netzwerke einsetzen. Falls ein Netzwerk Ihre DHCP-Anforderungen nicht erfüllt, müssen Sie die Netzwerke neu konfigurieren. Sie können Folgendes versuchen:

- Verwenden Sie eine Teilnetzmaske mit variabler Länge (Variable Length Subnet Mask, VLSM) in Ihren Teilnetzen, um den vorhandenen IP-Adressraum besser zu nutzen. Vermeiden Sie, mehrere Netzwerke im gleichen physikalischen Netzwerk auszuführen. Informationen zur Umsetzung von Teilnetzmasken mit variabler Länge finden Sie in der Manpage `netmasks(4)`. Ausführliche Informationen zu Classless Inter-Domain Routing (CIDR) und VLSM finden Sie unter `http://www.ietf.org/rfc/rfc1519.txt`.
- Konfigurieren Sie die Ports Ihrer Switches so, dass die Geräte unterschiedlichen physikalischen LANs zugewiesen werden. Diese Technik behält die Zuordnung eines LAN zu einem IP-Netzwerk bei, eine Voraussetzung für Oracle Solaris DHCP. Informationen zur Port-Konfiguration entnehmen Sie bitte der Dokumentation Ihres Switches.

Festlegen der Anzahl von DHCP-Servern

Die von Ihnen gewählte Datenspeicheroption hat direkte Auswirkungen auf die Anzahl der Server, die zur Unterstützung Ihrer DHCP-Clients erforderlich sind. Die folgende Tabelle zeigt die Höchstzahl an DHCP- und BOOTP-Clients, die von einem DHCP-Server für jeden Datenspeicher unterstützt werden können.

TABELLE 13–1 Geschätzte Höchstzahl an Clients, die von einem DHCP-Server unterstützt werden können

Datenspeichertyp	Höchstzahl der unterstützten Clients
Textdateien	10,000
NIS+	40,000
Binärdateien	100,000

Diese Höchstzahl ist eine allgemeine Richtlinie, keine absolute Zahl. Die Client-Kapazität eines DHCP-Servers hängt im Wesentlichen von der Anzahl der Transaktionen pro Sekunde ab, die der Server verarbeiten muss. Auch Leasing-Zeiten und Nutzungsmuster haben wesentlichen Einfluss auf die Transaktionsrate. Angenommen, Leasings sind auf 12 Stunden eingerichtet und die Benutzer schalten ihre Systeme über Nacht aus. Wenn dann viele Benutzer ihre Systeme morgens zur gleichen Zeit einschalten, muss der Server extrem viele Transaktionen abwickeln, da die zahlreiche Clients gleichzeitig Leasings anfordern. In einer solchen Umgebung kann der DHCP-Server weniger Clients unterstützen. In einer Umgebung mit längeren Leasing-Zeiten oder in einer Umgebung, die aus konstant verbundenen Geräten wie z. B. Kabelmodems besteht, kann der DHCP-Server mehr Clients unterstützen.

Die verschiedenen Datenspeichertypen werden im Abschnitt „Auswählen des DHCP-Datenspeichers“ auf Seite 343 miteinander verglichen.

Aktualisieren von Systemdateien und Netzmasken-Tabellen

Während der DHCP-Konfiguration scannen die DHCP-Tools verschiedene Systemdateien auf Ihrem Server nach Informationen, die zur Konfiguration des Servers verwendet werden können.

Aus diesem Grund müssen Sie vor dem Ausführen von DHCP Manager oder dem Befehl `dhcpconfig` zur Konfiguration Ihres Servers darauf achten, dass die Informationen in den Systemdateien auf dem neuesten Stand sind. Wenn Sie Fehler nach der Konfiguration des Servers bemerken, verwenden Sie DHCP Manager oder `dhtadm`, um die Makros auf dem Server zu modifizieren.

In der folgenden Tabelle sind einige der Informationen aufgeführt, die während der Konfiguration eines DHCP-Servers gesammelt wurden, sowie die Quellen dieser Informationen. Achten Sie darauf, dass diese Informationen korrekt auf dem Server eingerichtet wurden, bevor Sie mit der Konfiguration von DHCP auf dem Server beginnen. Wenn Sie Änderungen an den Systemdateien vornehmen, nachdem Sie den Server konfiguriert haben, müssen Sie den Service neu konfigurieren, um diese Änderungen widerzuspiegeln.

TABELLE 13–2 Informationen für die DHCP-Konfiguration

Informationen	Quelle	Bemerkungen
Zeitzone	Systemdatum, Zeitzoneneinstellungen	Datum und Zeitzone werden während der Oracle Solaris-Installation eingestellt. Sie können das Datum mithilfe des Befehls `date` ändern. Sie können die Zeitzone ändern, indem Sie in der Datei `/etc/default/init` die Umgebungsvariable `TZ` modifizieren. Weitere Informationen finden Sie in der Manpage `TIMEZONE(4)`.
DNS-Parameter	`/etc/resolv.conf`	Der DHCP-Server bezieht die NS-Parameter wie den DNS-Domänennamen und die DNS-Serveradressen aus der Datei `/etc/resolv.conf.` Weitere Informationen zur Datei `resolv.conf`finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* oder in der Manpage `resolv.conf(4)`.
NIS- oder NIS+-Parameter	System-Domänenname, `nsswitch.conf`, NIS oder NIS+	Der DHCP-Server bezieht den Domänennamen des Serversystems mit dem Befehl `domainname.` Die Datei `nsswitch.conf` weist den Server an, wo nach Domänen-basierten Informationen zu suchen ist. Handelt es sich bei dem Serversystem um einen NIS- oder NIS+-Client, führt der DHCP-Server eine Abfrage aus, um die IP-Adressen des NIS- oder NIS+-Servers zu erhalten. Weitere Informationen finden Sie in der Manpage `nsswitch.conf(4)`.
Standard-Router	System-Routing-Tabellen, Benutzeraufforderung	Der DHCP-Server durchsucht die Netzwerk-Routing-Tabellen, um den Standard-Router für Clients zu finden, die mit dem lokalen Netzwerk verbunden sind. Bei Clients, die sich nicht im gleichen Netzwerk befinden, fordert der DHCP-Server Informationen vom Benutzer an.

TABELLE 13–2 Informationen für die DHCP-Konfiguration *(Fortsetzung)*

Informationen	Quelle	Bemerkungen
Teilnetzmaske	Netzwerkschnittstelle, `netmasks`-Tabelle	Der DHCP-Server fragt seine eigenen Netzwerkschnittstellen ab, um die Netzmasken- und Broadcast-Adresse für lokale Clients zu ermitteln. Falls die Anforderung von einem Relay-Agent weitergeleitet wurde, bezieht der Server die Teilnetzmaske aus der `netmasks`-Tabelle im Netzwerk des Relay-Agent.
Broadcast-Adresse	Netzwerkschnittstelle, `netmasks`-Tabelle	Für das lokale Netzwerk bezieht der DHCP-Server die Broadcast-Adresse, indem er die Netzwerkschnittstelle abfragt. Bei remoten Netzwerken verwendet der Server die IP-Adresse des BOOTP-Relay-Agent und die Netzmaske des remoten Netzwerks, um die Broadcast-Adresse des Netzwerks zu berechnen.

Entscheidungen bei der Konfiguration Ihres DHCP-Servers (Übersicht der Schritte)

In diesem Abschnitt werden einige der Entscheidungen beschrieben, die Sie vor der Konfiguration des ersten DHCP-Servers im Ihrem Netzwerk treffen müssen. In der folgenden Tabelle finden Sie Informationen für die Konfiguration Ihres Netzwerks zur Verwendung von DHCP. Außerdem enthält die Tabelle Links zu den Abschnitten, in denen die Schritte für die Ausführung der Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
Auswählen eines Servers für DHCP.	Stellen Sie fest, ob ein Server die Systemvoraussetzungen zur Ausführung des DHCP-Services erfüllt.	„Auswählen eines Hosts zum Ausführen des DHCP-Services“ auf Seite 343
Auswählen eines Datenspeichers.	Vergleichen Sie die Datenspeichertypen und stellen Sie fest, welcher Datenspeicher am besten für Ihren Standort geeignet ist.	„Auswählen des DHCP-Datenspeichers“ auf Seite 343
Einrichten einer Leasing-Richtlinie.	Sammeln Sie Informationen zum Leasing von IP-Adressen, um die richtige Leasing-Richtlinie für Ihren Standort festzulegen.	„Einrichten einer Leasing-Richtlinie“ auf Seite 345

Aufgabe	Beschreibung	Siehe
Auswählen einer Router-Adresse oder Router-Erkennung.	Stellen Sie fest, ob DHCP-Clients die Router-Erkennung oder einen bestimmten Router verwendet.	„Festlegen der Router für DHCP-Clients“ auf Seite 346

Auswählen eines Hosts zum Ausführen des DHCP-Services

Unter Berücksichtigung Ihrer speziellen Netzwerktopologie können Sie die folgenden Systemvoraussetzungen verwenden, um einen Host auszuwählen, auf dem ein DHCP-Server eingerichtet werden soll.

Der Host muss die folgenden Voraussetzungen erfüllen:

- Der Host muss Solaris 2.6 oder eine aktuellere Version ausführen. Wenn Sie zahlreiche Clients unterstützen müssen, muss Solaris 8 7/01 oder eine aktuellere Version installiert sein.
- Der Host muss für alle Netzwerke zugänglich sein, in denen Clients vorhanden sind, die DHCP entweder direkt im Netzwerk oder über einen BOOTP-Relay-Agent verwenden sollen.
- Der Host muss zur Verwendung des Routings konfiguriert sein.
- Der Host muss über eine korrekt konfigurierte `netmasks`-Tabelle verfügen, in der Ihre Netzwerktopologie widergespiegelt wird.

Auswählen des DHCP-Datenspeichers

Sie können die DHCP-Daten in Textdateien, Binärdateien oder im NIS+-Verzeichnisdienst speichern. In der folgenden Tabelle sind die Eigenschaften jedes Datenspeichertyps zusammengefasst und es werden die Umgebungen aufgeführt, in denen jeder Datenspeichertyp am besten eingesetzt wird.

TABELLE 13–3 Vergleich der DHCP-Datenspeicher

Datenspeichertyp	Leistung	Wartungsaufwand	Gemeinsame Nutzung	Umgebung
Binärdateien	Hohe Leistung, hohe Kapazität	Geringer Wartungsaufwand, keine Datenbankserver erforderlich. Inhalte müssen mit DHCP Manager oder den Befehlen `dhtadm` und `pntadm` angezeigt werden. Regelmäßige Dateisicherungen sind empfohlen.	Datenspeicher können nicht mit anderen DHCP-Servern gemeinsam genutzt werden.	Mittelgroße bis große Umgebungen mit vielen Netzwerken mit tausenden von Clients pro Netzwerk. Geeignet für kleinere bis mittelgroße ISPs.
NIS+	Moderate Leistung und Kapazität, abhängig von Leistung und Kapazität des NIS+-Services	Das DHCP-Serversystem muss als ein NIS+-Client konfiguriert sein. Erfordert Pflege des NIS+-Services. Inhalte müssen mit DHCP Manager oder den Befehlen `dhtadm` und `pntadm` angezeigt werden. Regelmäßige Sicherungen mit dem Befehl `nisbackup` werden empfohlen.	DHCP-Daten sind in NIS+ verteilt, und mehrere Server können auf die gleichen Container zugreifen.	Kleine bis mittelgroße Umgebungen mit bis zu 5000 Clients pro Netzwerk.
Textdateien	Moderate Leistung, geringe Kapazität	Geringer Wartungsaufwand, keine Datenbankserver erforderlich. ASCII-Format ohne DHCP Manager, `dhtadm` oder `pntadm` lesbar. Regelmäßige Dateisicherungen sind empfohlen.	Der Datenspeicher kann mit mehreren DHCP-Servern gemeinsam genutzt werden, wenn die DHCP-Daten auf einem Dateisystem gespeichert werden, das über einen NFS-Einhängepunkt exportiert wird.	Kleine Umgebungen mit weniger als 10.000 Clients und 100 bis 1000 Clients pro Netzwerk.

Traditionelles NIS wird nicht als Datenspeicheroption angeboten, da NIS keine schnellen inkrementalen Aktualisierungen unterstützt. Falls NIS in Ihrem Netzwerk verwendet wird, sollten Sie Textdateien oder Binärdateien als Datenspeicher verwenden.

Einrichten einer Leasing-Richtlinie

Ein *Leasing* gibt an, wie lange es der DHCP-Server gestattet, dass ein DHCP-Client eine bestimmte IP-Adressen verwendet. Während der Erstkonfiguration des Servers geben Sie eine standortweit geltende Leasing-Richtlinie an. Die *Leasing-Richtlinie* legt die Leasing-Zeit fest und gibt an, ob Clients ihre Leasings erneuern können. Der Server verwendet die von Ihnen eingegebenen Informationen, um die Optionswerte in den Standardmakros einzurichten, die während der Konfiguration angelegt werden. Für bestimmte Clients oder Clienttypen können Sie unterschiedliche Leasing-Richtlinien einrichten, indem Sie die Optionen in den von Ihnen erstellten Konfigurationsmakros bearbeiten.

Die *Leasing-Zeit* wird in Stunden, Tagen oder Wochen angegeben, über die das Leasing gültig ist. Wenn einem Client eine IP-Adresse zugewiesen wird oder eine Leasing-Zeit für eine IP-Adresse neu ausgehandelt wird, werden das Ablaufdatum und die Leasing-Zeit berechnet. Die Anzahl an Stunden in der Leasing-Zeit wird dem Zeitstempel in der DHCP-Bestätigungsmeldung des Clients hinzugefügt. Angenommen, der Zeitstempel einer DHCP-Bestätigungsmeldung lautet September 16, 2005 9:15 A.M., und die Leasing-Zeit beträgt 24 Stunden. Das Leasing-Ablaufdatum und die -uhrzeit ist in diesem Fall 17. September 2005, 9:15 A.M. Das Leasing-Ablaufdatum wird im DHCP-Netzwerkdatensatz des Clients gespeichert und kann in DHCP Manager oder mit dem Dienstprogramm `pntadm` angezeigt werden.

Der Leasing-Zeitwert muss relativ klein sein, so dass abgelaufene Adressen schnell neu angefordert werden können. Andererseits muss der Leasing-Zeit wird groß genug sein, um Unterbrechungen des DHCP-Services zu überdauern. Clients müssen auch dann ordnungsgemäß arbeiten können, wenn das System, das den DHCP-Service ausführt, repariert wird. Eine allgemeine Richtlinie ist die Angabe einer Zeit, die doppelt so lang wie die erwartete Ausfallzeit eines Systems ist. Angenommen, Sie benötigen vier Stunden, um den defekten Teil eines Systems zu reparieren und das System neu zu starten, so geben Sie eine Leasing-Zeit von acht Stunden ein.

Mit der Option zur Aushandlung einer Leasing-Zeit wird festgelegt, ob ein Client seine Leasing-Zeit mit dem Server neu aushandeln kann, bevor das Leasing abläuft. Wenn Leasing-Aushandlungen gestattet sind, zeichnet der Client die verbleibende Leasing-Zeit auf. Ist die Leasing-Zeit halb verstrichen, fordert der Client den DHCP-Server auf, die Leasing-Zeit auf den ursprünglichen Wert zu verlängern. In Umgebungen mit mehr Systemen als IP-Adressen sollten Sie die Leasing-Aushandlung deaktivieren. In diesem Fall wird das Zeitlimit für die Verwendung der IP-Adressen durchgesetzt. Sind ausreichend IP-Adressen vorhanden, sollten Sie die Leasing-Aushandlung aktivieren, um so zu vermeiden, dass Clients gezwungen werden, ihre Netzwerkschnittstellen herunterzufahren, wenn Leasings ablaufen. Wenn Sie es gestatten, dass Clients neue Leasings beziehen, werden die TCP-Verbindungen des Clients, wie z. B. NFS und Telnet-Sitzungen, eventuell unterbrochen. Sie können die Leasing-Aushandlung für alle Clients während der Serverkonfiguration aktivieren. Mithilfe der Option `LeaseNeg` in Konfigurationsmakros können Sie die Leasing-Aushandlung auch nur für bestimmte Clients oder Clienttypen aktivieren.

Hinweis – Systeme, die dem Netzwerk Services bereitstellen, sollten ihre IP-Adressen behalten. Diesen Systemem sollten keine kurzen Leasings zugewiesen werden. Sie können DHCP mit diesen Systemen verwenden, wenn Sie ihnen manuell reservierte IP-Adressen anstelle von IP-Adressen mit permanenten Leasings zuweisen. In diesem Fall können Sie erkennen, wenn die IP-Adressen des Systems nicht mehr benutzt wird.

Festlegen der Router für DHCP-Clients

Hostsysteme verwenden Router für Netzwerkkommunikationen über das eigene lokale Netzwerk hinaus. Daher müssten Hosts die IP-Adressen dieser Router kennen.

Wenn Sie einen DHCP-Server konfigurieren, müssen Sie den DHCP-Clients die Router-Adressen in einer von zwei möglichen Methoden bereitstellen. Eine Möglichkeit ist es, den Routern bestimmte IP-Adressen zuzuweisen. Die bevorzugte Methode ist jedoch, dass Clients die Router mit dem Router Discovery-Protokoll erfassen.

Wenn Clients in Ihrem Netzwerk eine Router-Erkennung durchführen, sollten Sie das Router Discovery-Protokoll auch dann verwenden, wenn nur ein Router vorhanden ist. Mit der Router-Erkennung kann ein Client Router-Änderungen in einem Netzwerk leicht übernehmen. Angenommen, ein Router fällt aus und wird durch einen Router mit einer neuen Adresse ersetzt. In diesem Fall können Clients die neue Adresse automatisch erfassen, ohne dass eine neue Netzwerkkonfiguration erforderlich wird.

Entscheidungen bei der Verwaltung von IP-Adressen (Übersicht der Schritte)

Bei der Einrichtung des DHCP-Services müssen Sie verschiedene Aspekte von IP-Adressen festlegen, die der Server verwalten soll. Falls in Ihrem Netzwerk mehrere DHCP-Server erforderlich sind, können Sie jedem Server die Verantwortung über einen bestimmten IP-Adressbereich zuweisen. Sie müssen entscheiden, wie die Verantwortung für die Adressen aufgeteilt wird. In der folgenden Tabelle sind die Aufgaben aufgelistet, die Sie zur Verwaltung von IP-Adressen verwenden können, wenn Sie DHCP im Netzwerk einsetzen. Außerdem enthält die Tabelle Links zu den Abschnitten, in denen die Ausführung der einzelnen Aufgaben beschrieben ist.

Aufgabe	Beschreibung	Weitere Informationen
Festlegen, welche Adressen der Server verwalten soll.	Legen Sie fest, wie viele Adressen der DHCP-Server verwalten soll, und worum es sich bei diesen Adressen handelt.	„Anzahl und Bereiche der IP-Adressen“ auf Seite 347

Aufgabe	Beschreibung	Weitere Informationen
Festlegen, ob der Server automatisch Hostnamen für Clients erzeugen soll.	Ermitteln Sie, wie Hostnamen für Clients erzeugt werden, damit Sie entscheiden können, ob Hostnamen erzeugt werden sollen.	„Erzeugung des Client-Hostnamen" auf Seite 347
Festlegen des Konfigurationsmakros, das den Clients zugewiesen wird.	Erweitern Sie Ihre Kenntnisse zu den Client-Konfigurationsmakros, so dass Sie das für einen bestimmten Client geeigneten Makro auswählen können.	„Standardmäßige Client-Konfigurationsmakros" auf Seite 348
Festlegen des zu verwendenden Leasing-Typs.	Erweitern Sie Ihre Kenntnisse zu den Leasing-Typen, damit Sie festlegen können, welcher Typ für Ihre DHCP-Clients am besten geeignet ist.	„Dynamische und permanente Leasing-Typen" auf Seite 349

Anzahl und Bereiche der IP-Adressen

Während der Erstkonfiguration des Servers gestattet Ihnen DHCP Manager, einen Block (bzw. Bereich) an IP-Adressen unter der Verwaltung von DHCP hinzuzufügen, indem Sie die Gesamtzahl an Adressen und die erste Adresse im Block angeben. Anhand dieser Informationen fügt DHCP Manager eine Liste von aufeinander folgenden Adressen hinzu. Wenn Sie mehrere Blöcke von nicht aufeinander folgenden Adressen haben, können Sie die anderen Adressen durch erneutes Ausführen des Adress-Assistenten in DHCP Manager auch nach der Erstkonfiguration hinzufügen.

Bevor Sie Ihre IP-Adressen konfigurieren können, müssen Sie wissen, wie viele Adressen im ersten Adressblock enthalten sind, und wie die IP-Adresse der ersten Adresse im Bereich lautet, den Sie zuweisen möchten.

Erzeugung des Client-Hostnamen

Da DHCP ein dynamisches Protokoll ist, wird eine IP-Adresse nicht permanent dem Hostnamen des Systems zugeordnet, der sie momentan verwendet. Mit dem DHCP-Verwaltungstool können Sie einen Clientnamen erzeugen, der einer bestimmten IP-Adresse zugewiesen wird. Die Clientnamen bestehen aus einem Präfix bzw. Root-Namen plus einem Bindestrich und einer vom Server zugewiesene Zahl. Angenommen, der Root-Name lautet `charlie`, so lauten die Clientnamen `charlie-1`, `charlie-2`, `charlie-3` usw.

Standardmäßig beginnen die erzeugten Clientnamen mit dem Namen des DHCP-Servers, der sie verwaltet. Diese Strategie eignet sich besonders für Umgebungen, in denen mehrere DHCP-Server vorhanden sind, da Sie schnell aus den DHCP-Netzwerktabellen ersehen können, welche Clients von welchem DHCP-Server verwaltet werden. Sie können den Root-Namen jedoch auch in einen beliebigen benutzerdefinierten Namen ändern.

Bevor Sie mit der Konfiguration Ihre IP-Adressen beginnen, müssen Sie entscheiden, ob Sie die DHCP-Verwaltungstools zum Erzeugen von Clientnamen verwenden möchten, und wie der Root-Name für die Clientnamen in diesem Fall lauten soll.

Die erzeugten Clientnamen können in `/etc/inet/hosts`, DNS oder NIS+ zu IP-Adressen zugeordnet werden, wenn Sie die Hostnamen im Rahmen der DHCP-Konfiguration registrieren möchten. Weitere Informationen finden Sie unter „Registrierung des Client-Hostnamen“ auf Seite 385.

Standardmäßige Client-Konfigurationsmakros

In der Oracle Solaris DHCP-Terminologie ist ein *Makro* eine Sammlung von Netzwerkkonfigurationsoptionen und den diesen Optionen zugewiesenen Werten. Der DHCP-Server stellt anhand der Makros fest, welche Netzwerkkonfigurationsinformationen an einen DHCP-Client gesendet werden.

Wenn Sie den DHCP-Server konfigurieren, sammeln die Verwaltungstools Informationen aus Systemdateien, von Ihnen angegebene Befehlszeilenoptionen oder direkt über Eingabeaufforderungen. Anhand dieser Informationen erstellen die Verwaltungstools die folgenden Makros:

- **Netzwerkadresse-Makro** – das Netzwerkadresse-Makro erhält einen Namen, der der IP-Adresse des Clientnetzwerks entspricht. Angenommen, das Netzwerk ist `192.68.0.0`. Dann lautet der Name des Netzwerkadressenmakros ebenfalls `192.68.0.0`. Dieses Makro enthält Informationen, die von jedem Client im Netzwerk benötigt werden: Teilnetzmaske, Netzwerk-Broadcast-Adresse, Standard-Router oder Router Discovery-Token sowie NIS/NIS+-Domäne und Server, wenn der Server NIS/NIS+ verwendet. Eventuell sind auch andere Optionen enthalten, die für Ihr Netzwerk zutreffen. Das Netzwerkadresse-Makro wird automatisch für alle Clients verarbeitet, die sich in einem Netzwerk befinden. Lesen Sie dazu auch „Reihenfolge der Makroverarbeitung“ auf Seite 335.
- **Gebietsschema-Makro** – Der Name des Gebietsschema-Makros lautet `Locale`. Dieses Makro enthält den Offset (in Sekunden) von der Coordinated Universal Time (UTC), um die Zeitzone anzugeben. Das Gebietsschema-Makro wird nicht automatisch verarbeitet, aber es ist im Server-Makro enthalten.
- **Server-Makro** – Das Server-Makro erhält einen Namen, der dem Hostnamen des Servers gleicht. Angenommen, der Server heißt `pineola`. Dann lautet der Name des Server-Makros ebenfalls `pineola`. Das Server-Makro enthält Informationen zu Leasing-Richtlinie, Zeitserver, DNS-Domäne und DNS-Server sowie eventuell weitere Informationen, die das Konfigurationsprogramm aus den Systemdateien beziehen konnte. Das Server-Makro enthält das Gebietsschema-Makro, das heißt, der DHCP-Server verarbeitet das Gebietsschema-Makro als Teil des Server-Makros.

Wenn Sie die IP-Adressen für das erste Netzwerk konfigurieren, müssen Sie ein Client-Konfigurationsmakro auswählen, das für alle DHCP-Clients verwendet wird, die die von Ihnen konfigurierten Adressen verwenden. Das von Ihnen ausgewählte Makro wird den IP-Adressen zugeordnet. In der Standardeinstellung wird das Server-Makro ausgewählt, weil dieses Makro Informationen enthält, die von allen Clients, die diesen Server verwenden, benötigt werden.

Clients erhalten die im Netzwerkadresse-Makro enthaltenen Optionen vor den Optionen im Makro, die den IP-Adressen zugeordnet sind. Diese Verarbeitungsreihenfolge führt dazu, dass die Optionen im Server-Makro Vorrang vor allen eventuell widersprüchlichen Optionen im Netzwerkadresse-Makro haben. Weitere Informationen zur Verarbeitungsreihenfolge von Makros finden Sie unter „Reihenfolge der Makroverarbeitung“ auf Seite 335.

Dynamische und permanente Leasing-Typen

Der *Leasing-Typ* legt fest, ob die Leasing-Richtlinie für die von Ihnen konfigurierten IP-Adressen gilt. Mit DHCP Manager können Sie während der Erstkonfiguration des Servers entweder dynamische oder permanente Leasings für die von Ihnen hinzugefügten Adressen auswählen. Wenn Sie den DHCP-Server mit dem Befehl `dhcpconfig` konfigurieren, sind die Leasings dynamisch.

Hat eine IP-Adresse ein *dynamisches Leasing*, kann die Adresse vom DHCP-Server verwaltet werden. Der DHCP-Server kann die Art der IP-Adressen einem Client zuordnen, die Leasing-Zeit verlängern, erkennen, wenn die Adresse nicht mehr benötigt wird und die Adresse zurückfordern. Hat eine IP-Adresse ein *permanentes Leasing*, kann der DHCP-Server die Adresse nur zuweisen. Der Client ist dann Eigentümer dieser Adresse, bis er sie explizit wieder freigibt. Nachdem die Adresse freigegeben wurde, kann sie der Server einem anderen Client zuweisen. Wenn eine IP-Adresse als permanentes Leasing konfiguriert ist, unterliegt sie nicht der Leasing-Richtlinie.

Wenn Sie einen IP-Adressbereich konfigurieren, gilt der ausgewählte Leasing-Typ für alle Adressen im Bereich. Um bestmöglich von den Vorteilen von DHCP profitieren zu können, sollten Sie für den größten Teil der Adressen dynamische Leasings verwenden. Gegebenenfalls können Sie einzelne Adressen zu einem späteren Zeitpunkt bearbeiten, um sie in ein permanentes Leasing zu ändern. Die Gesamtzahl an permanenten Leasings sollte jedoch möglichst gering gehalten werden.

Reservierte IP-Adressen und Leasing-Typ

IP-Adressen können reserviert werden, indem sie bestimmten Clients manuell zugewiesen werden. Eine reservierte Adresse kann permanentem oder dynamischem Leasing zugewiesen werden. Wenn eine reservierte Adresse einem permanenten Leasing zugewiesen wird, treffen die folgenden Aussagen zu:

- Die Adresse kann nur dem Client zugewiesen werden, der an die Adresse gebunden ist.
- Der DHCP-Server kann die Adresse keinem anderen Client zuweisen.
- Die Adresse kann vom DHCP-Server nicht zurückgefordert werden.

Wenn eine reservierte Adresse einem dynamischen Leasing zugewiesen wird, kann die Adresse nur einem Client zugewiesen werden, der an die Adresse gebunden ist. Der Client muss die Leasing-Zeit jedoch aufzeichnen und eine Leasing-Verlängerung aushandeln, als wäre die Adresse nicht reserviert. Mit dieser Strategie können Sie verfolgen, wann der Client die Adresse verwendet. Dazu schlagen Sie einfach in der Netzwerktabellen nach.

Während der Erstkonfiguration können Sie nicht für alle IP-Adressen reservierte Adressen erstellen. Reservierte Adressen dürfen nur sparsam für einzelne Adressen eingesetzt werden.

Planung für mehrere DHCP-Server

Wenn Sie mehrere DHCP-Server zur Verwaltung Ihrer IP-Adressen konfigurieren möchten, müssen Sie die folgenden Richtlinien berücksichtigen:

- Teilen Sie den IP-Adresspool so auf, dass jeder Server für einen Adressbereich zuständig ist und dass es keine Überlappung bei den Bereichen gibt.
- Wählen Sie NIS+ als Datenspeichertyp, sofern verfügbar. Andernfalls wählen Sie Textdateien und geben ein gemeinsam genutztes Verzeichnis als absoluten Pfad zum Datenspeicher an. Ein Datenspeicher im Format Binärdateien kann nicht gemeinsam genutzt werden.
- Konfigurieren Sie jeden Server separat, so dass die Adresseigentümerschaft korrekt zugewiesen wird und Server-basierte Makros automatisch erstellt werden.
- Richten Sie die Server so ein, dass die Optionen und Makros in der Tabelle `dhcptab` in vorgegebenen Abständen gescannt werden, damit die Server die aktuellsten Informationen verwenden. Sie können DHCP Manager so einrichten, dass die `dhcptab`-Tabelle automatisch eingelesen wird. Lesen Sie dazu die Beschreibung unter „Anpassen der Leistungsoptionen für den DHCP-Server“ auf Seite 386.
- Achten Sie darauf, dass alle Clients auf alle DHCP-Server zugreifen können, so dass die Server einander unterstützen können. Ein Client mit einem gültigen Leasing für eine IP-Adresse könnte versuchen, seine Konfiguration zu überprüfen oder das Leasing zu verlängern, wenn der als Eigentümer der Clientadresse auftretende Server nicht erreichbar ist. In diesem Fall kann ein anderer Server auf die Clientanfragen reagieren, nachdem der

Client 20 Sekunden lang versucht hat, den primären Server zu kontaktieren. Hat ein Client eine bestimmte IP-Adresse angefordert, und ist der als Eigentümer der Clientadresse auftretende Server nicht erreichbar, kann einer der anderen Server die Anforderung bearbeiten. In diesem Fall erhält der Client die angeforderte Adresse nicht. Stattdessen erhält der Client eine IP-Adresse, die dem antwortenden DHCP-Server gehört.

Planung einer DHCP-Konfiguration für remote Netzwerke

Nach der DHCP-Erstkonfiguration können Sie IP-Adressen in remoten Netzwerken unter die DHCP-Verwaltung stellen. Da sich die Systemdateien jedoch nicht lokal auf dem Server befinden, können DHCP Manager und `dhcpconfig` keine Informationen nachschlagen, um Standardwerte bereitzustellen. Somit müssen Sie diese Informationen liefern. Bevor Sie versuchen, ein remotes Netzwerk zu konfigurieren, prüfen Sie, ob Sie über die folgenden Informationen verfügen:

- Die IP-Adresse des remoten Netzwerks.
- Die Teilnetzmaske des remoten Netzwerks. Diese Informationen können aus der `netmasks`-Tabelle des Namen-Services bezogen werden. Wenn das Netzwerk lokale Dateien verwendet, suchen Sie in der Datei `/etc/netmasks` auf einem System im Netzwerk. Wenn das Netzwerk NIS+ verwendet, geben Sie den Befehl `niscat netmasks.org_dir` ein. Wenn das Netzwerk NIS verwendet, geben Sie den Befehl `ypcat -k netmasks.byaddr` ein. Achten Sie darauf, dass die `netmasks`-Tabelle die Topologieinformationen aller von Ihnen verwalteten Teilnetze enthält.
- Den Netzwerktyp. Die Clients stellen die Verbindung zum Netzwerk entweder über eine LAN-Verbindung oder ein Point-to-Point-Protokoll (PPP) her.
- Routing-Informationen. Können die Clients die Router-Erkennung verwenden? Andernfalls müssen Sie die IP-Adresse eines Routers ermitteln, den die Clients verwenden können.
- NIS-Domäne und NIS-Server, falls anwendbar.
- NIS+-Domäne und NIS+-Server, falls anwendbar.

Informationen zu den Verfahren zum Hinzufügen von DHCP-Netzwerken finden Sie unter „Hinzufügen von DHCP-Netzwerken“ auf Seite 391.

Auswählen des Tools zur Konfiguration von DHCP

Nachdem Sie Informationen zusammengetragen und die Planungen für den DHCP-Service abgeschlossen haben, können Sie mit der Konfiguration eines DHCP-Servers beginnen. Zur Konfiguration eines Servers können Sie DHCP Manager oder das Befehlszeilenprogramm `dhcpconfig` verwenden. Mit DHCP Manager können Sie Optionen auszuwählen und Daten

angeben, die dann zum Erstellen der dhcptab- und der Netzwerktabellen verwendet werden, die von DHCP-Server abgefragt werden. Beim Dienstprogramm dhcpconfig verwenden Sie Befehlszeilenoptionen zur Angabe von Daten.

Funktionen von DHCP Manager

DHCP Manager, ein auf der Java™-Technologie basierendes GUI-Tool, enthält einen DHCP-Konfigurationsassistenten. Der Konfigurationsassistent wird automatisch gestartet, wenn Sie DHCP Manager das erste Mal auf einem System ausführen, das nicht als ein DHCP-Server konfiguriert ist. Der DHCP-Konfigurationsassistent zeigt eine Reihe von Dialogfelder an, in denen Sie zur Eingabe der zur Konfiguration eines Servers erforderlichen Informationen aufgefordert werden: Datenspeicherformat, Leasing-Richtlinie, DNS/NIS/NIS+ -Server und -Domänen sowie Routeradressen. Einige dieser Informationen bezieht der Assistent aus den Systemdateien, die Sie dann nur bestätigen oder gegebenenfalls korrigieren müssen.

Während Sie die Dialogfelder abarbeiten und die Informationen bestätigen, wird der DHCP-Serverdaemon auf dem Serversystem gestartet. Als Nächstes werden Sie aufgefordert, den Assistenten zum Hinzufügen von Adressen zu starten, um die IP-Adressen für das Netzwerk zu konfigurieren. Anfangs ist nur das Netzwerk des Servers für DHCP konfiguriert und die übrigen Serveroptionen erhalten Standardwerte. Sie können DHCP Manager nach der Erstkonfiguration erneut ausführen, um Netzwerke hinzuzufügen und andere Serveroptionen zu modifizieren.

Weitere Informationen zum DHCP-Konfigurationsassistenten finden Sie unter „Konfigurieren und Dekonfigurieren eines DHCP-Servers mithilfe von DHCP Manager“ auf Seite 356 Ausführliche Informationen zu DHCP Manager finden Sie unter „Allgemeines zum DHCP Manager“ auf Seite 368

dhcpconfig-Funktionen

Das Dienstprogramm dhcpconfig unterstützt Optionen, mit denen Sie einen DHCP-Server konfigurieren bzw. dekonfigurieren können. Außerdem können Sie einen neuen Datenspeicher konvertieren und Daten auf und von anderen DHCP-Server importieren bzw. exportieren. Wenn Sie das Dienstprogramm dhcpconfig zur Konfiguration eines DHCP-Servers verwenden, bezieht das Dienstprogramm Informationen aus den Systemdateien, die unter „Aktualisieren von Systemdateien und Netzmasken-Tabellen“ auf Seite 340 beschrieben sind. Sie können diese aus den Systemdateien bezogenen Informationen nicht wie mit DHCP-Manager anzeigen und bestätigen. Aus diesem Grund ist es wichtig, dass sich die Systemdateien auf dem neuesten Stand befinden, bevor Sie dhcpconfig ausführen. Werte in dhcpconfig, die Sie aus den Systemdateien bezogen haben, können Sie mit Befehlszeilenoptionen überschreiben. Der Befehl dhcpconfig kann nicht in Skripten verwendet werden. Weitere Informationen finden Sie in der Manpage dhcpconfig(1M).

Vergleich von DHCP Manager und `dhcpconfig`

In der folgenden Tabelle sind die Unterschiede zwischen den zwei Server-Konfigurationstools zusammengefasst.

TABELLE 13–4 Vergleich zwischen DHCP Manager und dem Befehl `dhcpconfig`

Funktion	DHCP Manager	`dhcpconfig` mit Optionen
Netzwerkinformationen werden vom System gesammelt.	Ermöglicht Ihnen das Anzeigen der aus den Systemdateien bezogenen Informationen und ggf. das Ändern dieser Informationen.	Sie können die Netzwerkinformationen mit Befehlszeilenoptionen angeben.
Konfigurationsgeschwindigkeit.	Beschleunigt den Konfigurationsprozess durch den Verzicht von Bestätigungen für weniger wichtige Serveroptionen. Stattdessen werden Standardwerte verwendet. Sie können weniger wichtige Optionen nach der Erstkonfiguration ändern.	Schnellster Konfigurationsprozess, aber eventuell müssen Sie Werte für viele Optionen angeben.

Kapitel 14, „Konfiguration des DHCP-Services (Aufgaben)“ enthält Verfahren, die Sie zur Konfiguration Ihres Servers mit DHCP-Manager oder dem Dienstprogramm `dhcpconfig` verwenden können.

KAPITEL 14

Konfiguration des DHCP-Services (Aufgaben)

Bei der Konfiguration des DHCP-Services in Ihrem Netzwerk konfigurieren und starten Sie den ersten DHCP-Server. Weitere DHCP-Server können zu einem späteren Zeitpunkt hinzugefügt werden. Sind die Daten an einem freigegebenen Speicherplatz abgelegt und unterstützt der Datenspeicher gemeinsamen Zugriff auf die Daten, können diese Server auf die gleichen Daten wie der erste Server zugreifen. In diesem Kapitel werden die Aufgaben beschrieben, mit denen Sie den DHCP-Server konfigurieren und die Netzwerke sowie deren zugewiesene IP-Adressen unter DHCP-Verwaltung konfigurieren. Darüber hinaus wird beschrieben, wie Sie einen DHCP-Server dekonfigurieren.

Jede Aufgabe umfasst ein Verfahren, wie Sie eine bestimmte Aufgabe in DHCP-Manager ausführen sowie ein Verfahren, die entsprechende Aufgabe mit dem Dienstprogramm `dhcpconfig` auszuführen. Dieses Kapitel enthält die folgenden Informationen:

- „Konfigurieren und Dekonfigurieren eines DHCP-Servers mithilfe von DHCP Manager" auf Seite 356
- „Konfigurieren und Dekonfigurieren eines DHCP-Servers mithilfe der `dhcpconfig`-Befehle" auf Seite 363

Falls Probleme bei der Konfiguration des DHCP-Services auftreten, lesen Sie Kapitel 17, „DHCP-Fehlerbehebung (Referenz)".

Nachdem Sie den DHCP-Service konfiguriert haben, lesen Sie Kapitel 15, „Verwalten von DHCP (Aufgaben)", in dem Sie weitere Informationen zur Verwaltung des DHCP-Services finden.

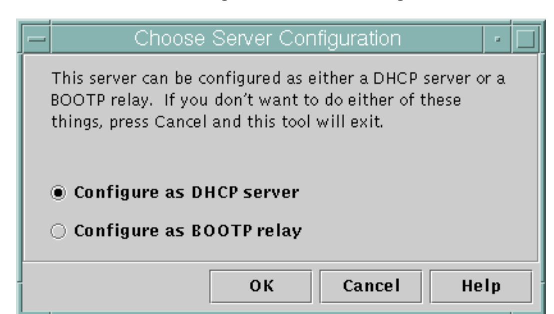
Konfigurieren und Dekonfigurieren eines DHCP-Servers mithilfe von DHCP Manager

Dieser Abschnitt enthält Verfahren, mit denen Sie einen DHCP-Server mit DHCP Manager konfigurieren und dekonfigurieren können. Beachten Sie, dass Sie zum Verwenden von DHCP-Server ein X-Window-System wie CDE oder GNOME ausführen müssen.

DHCP Manager kann mit dem Befehl `/usr/sadm/admin/bin/dhcpmgr` mit den Rechten eines Superusers ausgeführt werden. Allgemeine Informationen zu diesem Dienstprogramm finden Sie unter „Allgemeines zum DHCP Manager“ auf Seite 368 Ausführliche Informationen zum Ausführen von DHCP Manager finden Sie unter „So starten und stoppen Sie den DHCP-Service (DHCP Manager)“ auf Seite 373.

Wenn Sie DHCP Manager auf einem Server ausführen, der nicht für DHCP konfiguriert wurde, wird das folgende Dialogfeld angezeigt. Sie können angeben, ob ein DHCP-Server oder ein BOOTP-Relay-Agent konfiguriert werden soll.

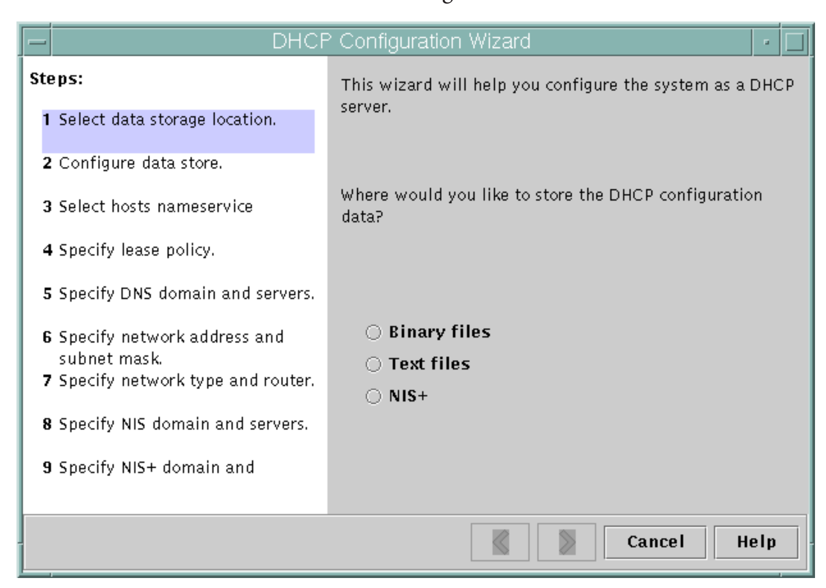
ABBILDUNG 14–1 Dialogfeld „ Serverkonfiguration auswählen“ in DHCP Manager



Konfiguration von DHCP-Servern

Wenn Sie einen DHCP-Server konfigurieren, startet DHCP Manager den DHCP-Konfigurationsassistent, der Sie zur Eingabe von Informationen auffordert, die zur Konfiguration des Servers erforderlich sind. Im Folgenden wird das erste Fenster des Assistenten gezeigt.

ABBILDUNG 14–2 Startfenster des DHCP-Konfigurationsassistenten



Nachdem Sie die Fragen des Assistenten beantwortet haben, erstellt DHCP Manager die in der folgenden Tabelle aufgeführten Objekte.

TABELLE 14–1 Während der DHCP-Serverkonfiguration erstellte Objektefüllen

Objekt	Beschreibung	Inhalte
Service-Konfigurationsdatei, `/etc/inet/dhcpsvc.conf`	Speichert Schlüsselwörter und Werte für die Server-Konfigurationsoptionen.	Datenspeichertyp und -speicherort sowie Optionen, die mit `in.dhcpd` verwendet werden, um den DHCP-Daemon beim Booten des Systems zu starten. Dieser Datei darf nicht manuell geändert werden. Zum Ändern der DHCP-Konfigurationsinformationen müssen Sie `dhcpmgr` oder `dhcpconfig` verwenden.
`dhcptab`-Tabelle	DHCP Manager erstellt eine `dhcptab`-Tabelle, falls diese Tabelle noch nicht existiert.	Makros und Optionen mit zugewiesenen Werten.
Gebietsschema-Makro (optional) mit der Bezeichnung `Locale`	Enthält den Offset der lokalen Zeitzone von der Universal Time (UTC) in Sekunden.	`UTCoffst`-Option mit einer zugewiesenen Zeit in Sekunden.

TABELLE 14–1 Während der DHCP-Serverkonfiguration erstellte Objektefüllen *(Fortsetzung)*

Objekt	Beschreibung	Inhalte
Servermakro, dessen Name dem Namen des Serverknotens entspricht	Enthält Optionen, deren Werte durch Eingaben des Administrators eingerichtet werden, der den DHCP-Server konfiguriert hat. Die Optionen gelten für alle Clients, die dem Server gehörende Adressen verwenden.	Das Makro `Locale` einschließlich der folgenden Optionen: ■ `Timeserv`, verweist auf die primäre IP-Adresse des Servers. ■ `LeaseTim`, gibt die Dauer für die Leasings in Sekunden an. ■ `LeaseNeg`, wenn Sie aushandelbare Leasings gewählt haben. ■ `DNSdmain` und `DNSserv`, wenn DNS konfiguriert wurde. ■ `Hostname`, dieser Option *darf kein* Wert zugewiesen werden. Das Vorhandensein dieser Option deutet darauf hin, dass der Hostname vom Namen-Service bezogen werden muss.
Netzwerkadresse-Makro, der Name für dieses Makro gleicht der Netzwerkadresse des Clientnetzwerks	Enthält Optionen, deren Werte durch Eingaben des Administrators eingerichtet werden, der den DHCP-Server konfiguriert hat. Die Optionen gelten für alle Clients, die sich in dem Netzwerk befinden, das durch den Makronamen angegeben wird.	Die folgenden Optionen: ■ `Subnet`, eingestellt auf die Teilnetzmaske des lokalen Teilnetzes ■ `Router`, eingestellt auf die IP-Adresse eines Router oder `RDiscvyF`, um den Client zu zwingen, die Router-Erkennung zu verwenden ■ `Broadcst`, eingestellt auf die Broadcast-IP-Adresse. Diese Option ist nur dann vorhanden, wenn es sich bei dem Netzwerk nicht um ein Point-to-Point-Netzwerk handelt. ■ `MTU`, für die maximale Übertragungseinheit ■ `NISdmain` und `NISservs`, falls NIS konfiguriert ist ■ `NIS+dom` und `NIS+serv`, falls NIS+ konfiguriert ist
Netzwerktabelle für das Netzwerk	Es wird eine leere Tabelle erstellt, bis Sie IP-Adressen für das Netzwerk zuweisen.	Kein Inhalt, bis Sie IP-Adressen hinzufügen.

▼ So konfigurieren Sie einen DHCP-Server (DHCP Manager)

Bevor Sie beginnen Bevor Sie mit der Konfiguration Ihres DHCP-Servers beginnen, sollten Sie Kapitel 13, „Planungen für den DHCP-Service (Aufgaben)“ lesen. Achten Sie besonders auf die Richtlinien unter „Entscheidungen bei der Konfiguration Ihres DHCP-Servers (Übersicht der Schritte)“ auf Seite 342, die Sie bei den folgenden Aufgaben unterstützen:

- Auswählen des Systems, das als DHCP-Server verwendet werden soll.
- Treffen von Entscheidungen hinsichtlich Datenspeicher, Leasing-Richtlinie und Router-Informationen.

1. **Melden Sie sich beim Serversystem als Superuser an.**

2. **Starten Sie DHCP Manager.**

   ```
   #/usr/sadm/admin/bin/dhcpmgr &
   ```

3. **Wählen Sie die Option „Als DHCP-Server konfigurieren“.**

   Der DHCP-Konfigurationsassistent wird gestartet und unterstützt Sie bei der Konfiguration Ihres Servers.

4. **Basierend auf den Entscheidungen, die Sie in der Planungsphase getroffen haben, wählen Sie Optionen aus oder geben angeforderten Informationen ein.**

   Falls Probleme auftreten, klicken Sie im Fenster des Assistenten auf „Hilfe“, um Ihren Webbrowser zu öffnen und die Hilfe für den DHCP-Konfigurationsassistenten anzuzeigen.

5. **Klicken Sie auf „Fertig stellen“, um die Serverkonfiguration abzuschließen, nachdem Sie alle erforderlichen Informationen eingegeben haben.**

6. **Klicken Sie bei der Eingabeaufforderung „Adressassistent starten“ auf „Ja“, um die IP-Adressen für den Server zu konfigurieren.**

   Mit dem Assistenten „Adressen zum Netzwerk hinzufügen“ können Sie angeben, welche Adressen unter die DHCP-Verwaltung gestellt werden sollen.

7. **Beantworten Sie die Eingabeaufforderungen entsprechend den Entscheidungen, die Sie während der Planungsphase getroffen haben.**

   Weitere Informationen finden Sie unter „Entscheidungen bei der Verwaltung von IP-Adressen (Übersicht der Schritte)“ auf Seite 346. Falls Probleme auftreten, klicken Sie im Fenster des Assistenten auf „Hilfe“, um Ihren Webbrowser zu öffnen und die Hilfe für den Assistenten „Adressen zum Netzwerk hinzufügen“ anzuzeigen.

8 **Überprüfen Sie Ihre Auswahl, dann klicken Sie auf „Fertig stellen", um die IP-Adressen zur Netzwerktabelle hinzuzufügen.**

Die Netzwerktabelle wird mit Datensätzen für jede Adresse in dem von Ihnen angegebenen Bereich aktualisiert.

Siehe auch Mit dem Netzwerk-Assistenten können Sie weitere Netzwerke zum DHCP-Server hinzufügen. Dies wird unter „Hinzufügen von DHCP-Netzwerken" auf Seite 391 beschrieben.

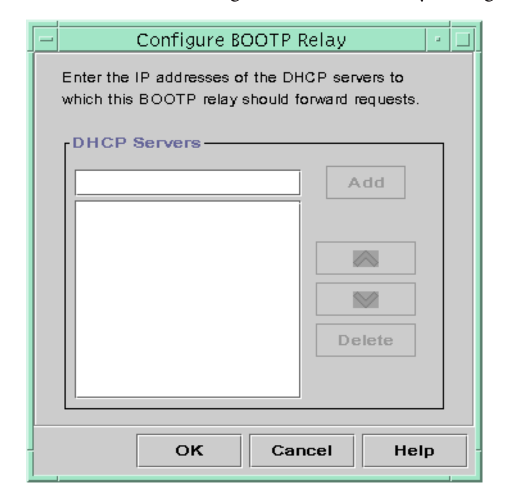
Konfiguration eines BOOTP-Relay-Agent

Bei der Konfiguration eines BOOTP-Relay-Agent führt DHCP Manager die folgenden Aktionen aus:

- Sie werden zur Eingabe der IP-Adressen eines oder mehrerer DHCP-Server aufgefordert, an die Anforderungen weitergeleitet werden sollen
- Die Einstellungen für den BOOTP-Relay-Service werden gespeichert

Das folgende Fenster wird angezeigt, wenn Sie die Konfiguration eines BOOTP-Relay-Agent auswählen.

ABBILDUNG 14–3 Dialogfeld „BOOTP-Relay konfigurieren" in DHCP Manager



▼ So konfigurieren Sie einen BOOTP-Relay-Agent (DHCP Manager)

Bevor Sie beginnen Bevor Sie mit der Konfiguration Ihres BOOTP-Relay-Agenten beginnen, sollten Sie Kapitel 13, „Planungen für den DHCP-Service (Aufgaben)“ lesen. Insbesondere sollten Sie „Auswählen eines Hosts zum Ausführen des DHCP-Services“ auf Seite 343 gelesen haben, da Sie in diesem Abschnitt Informationen zur Auswahl des zu verwendenden Systems finden.

1. **Melden Sie sich beim Serversystem als Superuser an.**

2. **Starten Sie DHCP Manager.**

```
#/usr/sadm/admin/bin/dhcpmgr &
```

Falls das System weder als DHCP-Server noch als BOOTP-Relay-Agent konfiguriert ist, startet der DHCP-Konfigurationsassistent. Wenn das System bereits als ein DHCP-Server konfiguriert wurde, müssen Sie den Server zunächst dekonfigurieren. Lesen Sie dazu „Dekonfiguration von DHCP-Servern und BOOTP-Relay-Agents“ auf Seite 361.

3. **Wählen Sie „Als BOOTP-Relay konfigurieren“.**

Das Dialogfeld „BOOTP-Relay konfigurieren“ wird angezeigt.

4. **Geben Sie die IP-Adresse oder den Hostnamen eines oder mehrerer DHCP-Server ein, und klicken Sie auf „Hinzufügen“.**

Die angegebenen DHCP-Server müssen zur Verarbeitung von BOOTP- oder DHCP-Anforderungen konfiguriert sein, die von diesem BOOTP-Relay-Agent empfangen werden.

5. **Klicken Sie auf „OK“, um das Dialogfeld zu schließen.**

Beachten Sie, dass DHCP Manager jetzt neue Menüs anzeigt: das Menü „Datei“, über das Sie die Anwendung beenden können, und das Menü „Service“ über das Sie den Server verwalten können. Die deaktivierten Menüoptionen eignen sich nur für einen DHCP-Server.

Dekonfiguration von DHCP-Servern und BOOTP-Relay-Agents

Wenn Sie einen DHCP-Server oder BOOTP-Relay-Agent dekonfigurieren, führt DHCP Manager die folgenden Aktionen aus:

- Der DHCP-Daemon (`in.dhpcd`) wird angehalten
- Die Datei `/etc/inet/dhcpsvc.conf`, in der Informationen zum Starten des Daemon sowie zum Speicherort des Datenspeichers aufgezeichnet werden, wird gelöscht

Das folgende Fenster wird angezeigt, wenn Sie einen DHCP-Server dekonfigurieren.

ABBILDUNG 14–4 Dialogfeld „Service dekonfigurieren“ in DHCP Manager

Unconfigure Service

Are you sure it is OK to unconfigure the DHCP service? If you are using a shared data store such as NIS+, removing the dhcptab and network tables may affect other DHCP servers.

Remove the dhcptab and all DHCP network tables

Remove all hosts table entries for DHCP addresses

DHCP Manager will exit once the service has been unconfigured.

OK Cancel Help

DHCP-Daten auf einem dekonfigurierten Server

Wenn ein DHCP-Server dekonfiguriert werden soll, müssen Sie entscheiden, was mit der `dhcptab`-Tabelle und den DHCP-Netzwerktabellen geschehen soll. Wenn die Daten von mehreren Servern gemeinsam genutzt werden, dürfen Sie die `dhcptab`-Tabelle und die DHCP-Netzwerktabellen nicht löschen. Wenn diese Tabellen gelöscht werden, kann DHCP nicht mehr in Ihrem Netzwerk verwendet werden. Die Daten können über NIS+ oder über exportierte lokale Dateisysteme freigegeben werden. Der verwendete Datenspeicher sowie dessen Speicherort wird in der Datei `/etc/inet/dhcpsvc.conf` aufgezeichnet.

Sie können einen DHCP-Server dekonfigurieren und die Daten intakt lassen, indem Sie keine der Optionen zum Löschen der Daten auswählen. Wenn Sie den Server dekonfigurieren und die Daten intakt lassen, deaktivieren Sie den DHCP-Server.

Wenn ein anderer DHCP-Server die Eigentümerschaft über die IP-Adressen übernehmen soll, müssen Sie die DHCP-Daten auf diesen anderen DHCP-Server verschieben. Die Daten müssen verschoben werden, bevor Sie den aktuellen Server dekonfigurieren. Weitere Informationen finden Sie unter „Verschieben von Konfigurationsdaten zwischen DHCP-Servern (Übersicht der Schritte)“ auf Seite 446.

Wenn Sie sicher sind, dass die Daten gelöscht werden sollen, können Sie eine der Optionen zum Löschen der `dhcptab`-Tabelle und der Netzwerktabellen wählen. Haben Sie Clientnamen für die DHCP-Adressen erzeugt, können Sie auch diese Einträge aus der hosts-Tabelle entfernen. Einträge von Clientnamen können aus DNS, `/etc/inet/hosts` oder NIS+ entfernt werden.

Bevor Sie einen BOOTP-Relay-Agent dekonfigurieren, müssen ein Sie sicherstellen, dass keine Clients diesen Agenten verwenden, um Anforderungen an einen DHCP-Server weiterzuleiten.

▼ So dekonfigurieren Sie einen DHCP-Server oder einen BOOTP-Relay-Agent (DHCP Manager)

1 Melden Sie sich als Superuser an.

2 Starten Sie DHCP Manager.

```
#/usr/sadm/admin/bin/dhcpmgr &
```

3 Wählen Sie im Menü „Service" die Option „Dekonfigurieren" aus.

Das Dialogfeld „Service dekonfigurieren" wird angezeigt. Handelt es sich bei dem Server um einen BOOTP-Relay-Agent, können Sie im Dialogfeld bestätigen, dass Sie den Relay-Agent dekonfigurieren möchten. Handelt es sich bei dem Server um einen DHCP-Server, müssen Sie zunächst entscheiden, was mit den DHCP-Daten geschehen soll, dann treffen Sie eine Auswahl im Dialogfeld. Siehe dazu Abbildung 14–4.

4 (Optional) Wählen Sie Optionen zum Löschen von Daten.

Wenn der Server gemeinsam genutzte Daten über NIS+ oder in Dateien nutzt, die über NFS freigegeben sind, dürfen Sie keine der Optionen zum Löschen der Daten wählen. Verwendet der Server keine gemeinsam genutzten Daten, können Sie eine oder beide Optionen zum Löschen der Daten wählen.

Weitere Informationen zum Löschen von Daten finden Sie unter „DHCP-Daten auf einem dekonfigurierten Server" auf Seite 362.

5 Klicken Sie auf „OK", um den Server zu dekonfigurieren.

Das Dialogfeld „Service dekonfigurieren" und DHCP Manager werden geschlossen.

Konfigurieren und Dekonfigurieren eines DHCP-Servers mithilfe der `dhcpconfig`-Befehle

Dieser Abschnitt enthält Verfahren, mit denen Sie einen DHCP-Server oder einen BOOTP-Relay-Agent mithilfe der `dhcpconfig`-Befehlszeilenoptionen konfigurieren oder dekonfigurieren können.

▼ So konfigurieren Sie einen DHCP-Server (dhcpconfig -D)

Bevor Sie beginnen Bevor Sie mit der Konfiguration Ihres DHCP-Servers beginnen, sollten Sie Kapitel 13, „Planungen für den DHCP-Service (Aufgaben)" lesen. Achten Sie besonders auf die Richtlinien unter „Entscheidungen bei der Konfiguration Ihres DHCP-Servers (Übersicht der Schritte)" auf Seite 342, die Sie bei den folgenden Aufgaben unterstützen:

- Auswählen des Systems, das als DHCP-Server verwendet werden soll.
- Treffen von Entscheidungen hinsichtlich Datenspeicher, Leasing-Richtlinie und Router-Informationen.

1. **Melden Sie sich bei dem System, auf dem der DHCP-Server konfiguriert werden soll, als Superuser an.**

2. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

3. **Konfigurieren Sie den DHCP-Server, in dem Sie einen Befehl mit der folgenden Syntax eingeben:**

   #/usr/sbin/dhcpconfig -D -r *datastore* **-p** *location*

   Datenspeicher isi einer der Folgenden: SUNWfiles , SUNWbinfiles oder SUNWnisplus.

   Speicherort ist der Datenspeicher-abhängige Speicherort, an dem Sie die DHCP-Daten speichern. Bei SUNWfiles und SUNWbinfiles muss der Speicherort mit einem absoluten Pfadnamen angegeben werden. Bei SUNWnisplus muss der Speicherort ein vollständig angegebenes NIS+-Verzeichnis sein.

   Sie können z. B. einen Befehl ähnlich dem Folgenden eingegeben:

   ```
   dhcpconfig -D -r SUNWbinfiles -p /var/dhcp
   ```

   Das Dienstprogramm dhcpconfig verwendet die Host-Systemdateien und Netzwerkdateien, um die zur Konfiguration des DHCP-Servers erforderlichen Werte zu ermitteln. Weitere Informationen zu den zusätzlichen Optionen für den Befehl dhcpconfig, mit denen Sie die Standardwerte außer Kraft setzen können, finden Sie in der Manpage dhcpconfig(1M).

4. **Fügen Sie dem DHCP-Service eines oder mehrere Netzwerke hinzu.**

   Informationen zum Hinzufügen eines Netzwerks finden Sie unter „So fügen Sie ein DHCP-Netzwerk hinzu (dhcpconfig)" auf Seite 393.

▼ So konfigurieren Sie einen BOOTP-Relay-Agent (`dhcpconfig -R`)

Bevor Sie beginnen Wählen Sie das System, das als BOOTP-Relay-Agent verwendet werden soll. Nutzen Sie dabei die unter „Auswählen eines Hosts zum Ausführen des DHCP-Services“ auf Seite 343 aufgeführten Anforderungen.

1. **Melden Sie sich bei dem Server an, den Sie als BOOTP-Relay-Agent konfigurieren möchten.**

2. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

3. **Konfigurieren Sie den BOOTP-Relay-Agent, in dem Sie einen Befehl mit der folgenden Syntax eingeben:**

   `# /usr/sbin/dhcpconfig -R` *server-addresses*

   Geben Sie eine oder mehrere IP-Adressen der DHCP-Server ein, an den bzw. die Anforderungen weitergeleitet werden sollen. Trennen Sie mehrere Adressen durch Kommata.

   Sie können z. B. einen Befehl ähnlich dem Folgenden eingegeben:

```
/usr/sbin/dhcpconfig -R 192.168.1.18,192.168.42.132
```

▼ So dekonfigurieren Sie einen DHCP-Server oder einen BOOTP-Relay-Agent (`dhcpconfig -U`)

1. **Melden Sie sich bei dem DHCP-Server oder BOOTP-Relay-Agent-System an, dessen Konfiguration rückgängig gemacht werden soll.**

2. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

3 Dekonfigurieren Sie den DHCP-Server oder den BOOTP-Relay-Agent:

```
# /usr/sbin/dhcpconfig -U
```

Wenn der Server keine gemeinsam genutzten Daten verwendet, geben Sie die Option `-x` ein, um die `dhcptab`-Tabelle und die Netzwerktabellen zu löschen. Wenn der Server gemeinsam genutzte Daten verwendet, dürfen Sie die Option `-x` nicht verwenden. Mit der Option `-h` werden Hostnamen aus der hosts-Tabelle gelöscht. Weitere Informationen zu den Optionen von `dhcpconfig` finden Sie in der Manpage `dhcpconfig`(1M).

Weitere Informationen zum Löschen von Daten finden Sie unter „DHCP-Daten auf einem dekonfigurierten Server“ auf Seite 362.

KAPITEL 15

Verwalten von DHCP (Aufgaben)

In diesem Kapitel werden Aufgaben beschrieben, die Sie bei der Verwaltung des Oracle Solaris DHCP-Service unterstützen. Dieses Kapitel enthält Aufgaben für den Server, den BOOTP-Relay-Agent und den Client. Jede Aufgabe enthält ein Verfahren, wie Sie eine bestimmte Aufgabe in DHCP Manager ausführen, sowie ein Verfahren, wie Sie die gleiche Aufgabe mit den DHCP-Befehlszeilenprogrammen ausführen. In die DHCP-Befehlszeilenprogramme sind in Manpages ausführlicher beschrieben.

Bevor Sie die Aufgaben in diesem Kapitel durchführen, müssen Sie die Erstkonfiguration des DHCP-Services und des Netzwerks durchgeführt haben. Die DHCP-Konfiguration wird in Kapitel 14, „Konfiguration des DHCP-Services (Aufgaben)" beschrieben.

Dieses Kapitel enthält die folgenden Informationen:

- „Allgemeines zum DHCP Manager" auf Seite 368
- „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371
- „Starten und Stoppen des DHCP-Service" auf Seite 372
- „DHCP-Service und die Service Management Facility" auf Seite 374
- „Bearbeiten von DHCP-Service-Optionen (Übersicht der Schritte)" auf Seite 375
- „Hinzufügen, Modifizieren und Löschen von DHCP-Netzwerken (Übersicht der Schritte)" auf Seite 388
- „Unterstützen von BOOTP-Clients mit dem DHCP-Service (Übersicht der Schritte)" auf Seite 399
- „Arbeiten mit IP-Adressen im DHCP-Service (Übersicht der Schritte)" auf Seite 402
- „Arbeiten mit DHCP-Makros (Übersicht der Schritte)" auf Seite 419
- „Arbeiten mit DHCP-Optionen (Übersicht der Schritte)" auf Seite 430
- „Unterstützung der Oracle Solaris-Netzwerkinstallation mit dem DHCP-Service" auf Seite 440
- „Unterstützung von remten Booten und laufwerkslosen Boot-Clients (Übersicht der Schritte)" auf Seite 440
- „Einrichten von DHCP-Clients ausschließlich zum Empfang von Informationen (Übersicht der Schritte)" auf Seite 442
- „Umwandeln des DHCP-Datenspeicherstyps" auf Seite 443

- „Verschieben von Konfigurationsdaten zwischen DHCP-Servern (Übersicht der Schritte)“ auf Seite 446

Allgemeines zum DHCP Manager

DHCP Manager ist ein Tool mit grafischer Benutzeroberfläche (GUI), mit dem Sie alle Verwaltungsaufgaben durchführen können, die dem DHCP-Service zugeordnet sind.

Fenster „DHCP Manager“

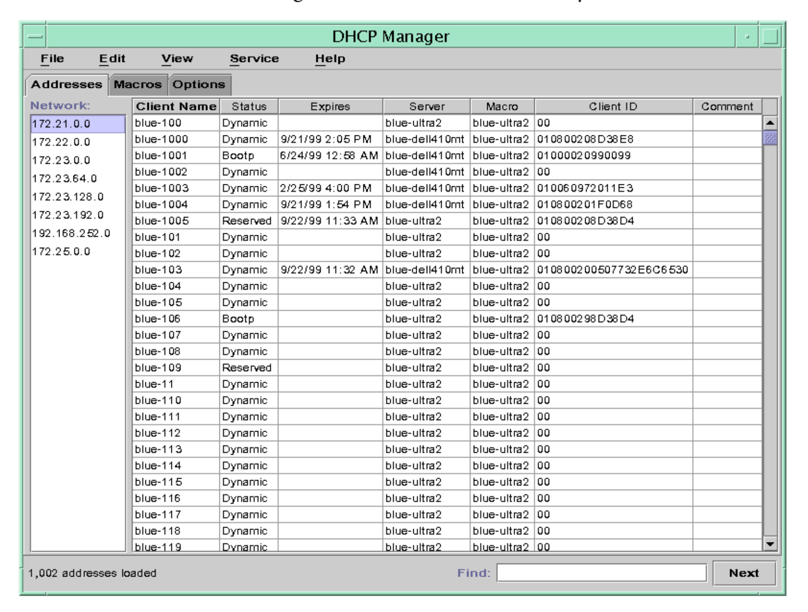
Das Erscheinungsbild der DHCP Manager-Fenster hängt davon ab, wie der DHCP-Server auf dem System konfiguriert ist, auf dem DHCP Manager ausgeführt wird.

DHCP Manager verwendet auf Registerkarten basierende Fenster, wenn das System als DHCP-Server konfiguriert ist. Sie wählen eine Registerkarte für die Informationen, mit denen Sie arbeiten möchten. DHCP Manager umfasst die folgenden Registerkarten:

- **Adressen** – Auf dieser Registerkarte werden alle Netzwerke und IP-Adressen aufgeführt, die unter die Verwaltung von DHCP gestellt wurden. Auf der Registerkarte „Adressen“ können Sie mit Netzwerken und IP-Adressen arbeiten. Sie können einzelne Objekte oder Blöcke hinzufügen oder löschen. Sie können auch die Eigenschaften einzelner Netzwerke oder IP-Adressen ändern oder die gleichen Änderungen an einem Adressblock vornehmen. Wenn Sie DHCP Manager starten, wird zunächst die Registerkarte „Adressen“ angezeigt.
- **Makros** – Auf dieser Registerkarte sind alle verfügbaren Makros in der DHCP-Konfigurationstabelle (`dhcptab`) sowie die in diesen Makros enthaltenen Optionen aufgeführt. Auf der Registerkarte „Makros“ können Sie Makros erstellen oder löschen. Darüber hinaus können Sie Makros bearbeiten, indem Sie Optionen hinzufügen und Werte für diese Optionen angeben.
- **Optionen** – Auf dieser Registerkarte sind alle Optionen aufgeführt, die für diesen DHCP-Server definiert wurden. Die auf dieser Registerkarte aufgeführten Optionen sind keine im DHCP-Protokoll definierten Standardoptionen. Die Optionen sind Erweiterungen der Standardoptionen und gehören der Klasse Erweitert, Hersteller oder Standort an. Standardoptionen können nicht geändert werden, daher werden diese Optionen hier nicht aufgeführt.

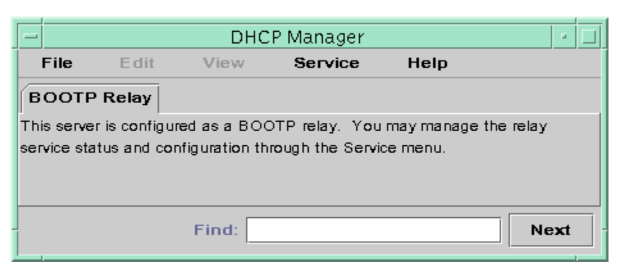
Die folgende Abbildung zeigt ein mögliches Erscheinungsbild des Fensters „DHCP Manager“, wenn Sie DHCP Manager auf einem DHCP-Server starten.

ABBILDUNG 15–1 DHCP Manager auf einem DHCP-Server-System



Wenn der Server als BOOTP-Relay-Agent konfiguriert wurde, zeigt das Fenster „DHCP Manager“ keine Registerkarten an. Ein BOOTP-Relay-Agent benötigt diese Informationen nicht. Sie können lediglich die Eigenschaften des BOOTP-Relay-Agent ändern und den DHCP-Daemon mit DHCP Manager starten oder stoppen. Die folgende Abbildung zeigt, wie DHCP Manager auf einem System aussieht, das als BOOTP-Relay-Agent konfiguriert ist.

ABBILDUNG 15–2 DHCP Manager auf einem BOOTP-Relay-Agent



Menüs in DHCP Manager

Die Menüs in DHCP Manager enthalten die folgenden Optionen:

- **Datei** – Beenden von DHCP Manager.
- **Bearbeiten** – Durchführen von Verwaltungsaufgaben für Netzwerke, Adressen, Makros und Optionen.
- **Ansicht** – Ändern des Erscheinungsbilds der derzeit ausgewählten Registerkarte.
- **Service** – Verwalten des DHCP-Daemon und des Datenspeichers.
- **Hilfe** – Öffnen Ihres Webbrowsers und Anzeigen der Hilfe für DHCP Manager.

Wenn DHCP Manager auf einem BOOTP-Relay-Agent ausgeführt wird, sind die Menüs „Bearbeiten" und „Ansicht" deaktiviert.

Alle Aufgaben zu DHCP-Verwaltung werden über die Menüs „Bearbeiten" und „Service" abgewickelt.

Mit den Befehlen im Menü „Bearbeiten" können Sie Objekte auf der gewählten Registerkarte erstellen, löschen und modifizieren. Bei den Objekten kann es sich um Netzwerke, Adressen, Makros oder Optionen handeln. Wenn die Registerkarte „Adressen" ausgewählt ist, enthält das Menü „Bearbeiten" auch Assistenten. Assistenten sind eine Reihe von Dialogfeldern, die Ihnen dabei helfen, Netzwerke und mehrere IP-Adressen zu erstellen.

Mit den Befehlen im Menü „Service" können Sie den DHCP-Daemon verwalten. Mit den Befehlen im Menüs „Service" können Sie Folgendes:

- Den DHCP-Daemon starten und stoppen.
- Den DHCP-Daemon aktivieren und deaktivieren.
- Die Serverkonfiguration modifizieren.
- Den Server dekonfigurieren.
- Den Datenspeicher konvertieren.
- Daten auf dem Server importieren und exportieren.

Starten und Stoppen von DHCP Manager

Zum Ausführen von DHCP Manager auf einem DHCP-Serversystem müssen Sie als Superuser angemeldet sein. Wenn Sie DHCP Manager standortfern ausführen müssen, können Sie die Anzeige mithilfe der Remote-Anzeigefunktion „X Window" an Ihr System umleiten lassen.

▼ So starten und stoppen Sie DHCP Manager

1 Melden Sie sich als Superuser beim DHCP-Serversystem an.

2 (Optional) Wenn Sie sich die standortfern beim DHCP-Serversystem angemeldet haben, können Sie DHCP Manager auf Ihrem lokalen System anzeigen. Dazu führen Sie die folgenden Schritte aus.

a. Geben Sie Folgendes auf dem lokalen System ein:

```
# xhost +server-name
```

b. Geben Sie Folgendes auf dem remoten DHCP-Serversystem ein:

```
# DISPLAY=local-hostname;export DISPLAY
```

3 Starten Sie DHCP Manager.

```
# /usr/sadm/admin/bin/dhcpmgr &
```

Das Fenster „DHCP Manager" wird geöffnet. Wenn der Server als DHCP-Server konfiguriert ist, zeigt das Fenster die Registerkarte „Adressen" an. Ist der Server als BOOTP-Relay-Agent konfiguriert, enthält das Fenster keine Registerkarten.

4 Um DHCP Manager zu stoppen, wählen Sie „Beenden" im Menü „Datei" aus.

Das Fenster „DHCP Manager" wird geschlossen.

Einrichten des Benutzerzugriffs auf DHCP-Befehle

In der Standardeinstellung kann nur ein Root- oder Superuser die Befehle `dhcpconfig`, `dhtadm` und `pntadm` ausführen. Wenn Sie möchten, dass Benutzer ohne Root-Berechtigungen diese Befehle verwenden können, müssen Sie eine rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC) einrichten.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

Eventuell sind auch die Informationen in den folgenden Manpages für Sie hilfreich: `rbac(5)`, `exec_attr(4)` und `user_attr(4)`.

Im folgenden Verfahren wird beschrieben, wie Sie das DHCP Management-Profil zuweisen, das einen Benutzer berechtigt, DHCP-Befehle auszuführen.

▼ So gewähren Sie Benutzern Zugriff auf DHCP-Befehle

1 Melden Sie sich als Superuser beim DHCP-Serversystem an.

2. **Fügen Sie der Datei `/etc/user_attr` einen Befehl in der folgenden Syntax hinzu. Fügen Sie einen Eintrag für jeden Benutzer bzw. jede Rolle hinzu, die den DHCP-Service verwalten darf.**

   username`:::type=normal;profiles=DHCP Management`

   Für den Benutzer `ram` fügen Sie z. B. den folgenden Eintrag hinzu:

   ```
   ram:::type=normal;profiles=DHCP Management
   ```

Starten und Stoppen des DHCP-Service

In diesem Abschnitt wird beschrieben, wie Sie den DHCP-Service mithilfe von DHCP Manager und dem Befehl `dhcpconfig` starten bzw. stoppen. Der DHCP-Service kann auch mithilfe der Service Management Facility (SMF)-Befehle gestartet bzw. gestoppt werden. Weitere Informationen zum Verwenden von SMF-Befehlen mit dem DHCP-Service finden Sie unter „DHCP-Service und die Service Management Facility" auf Seite 374.

Das Starten bzw. Stoppen des DHCP-Service umfasst verschiedene Aktionen, mit denen Sie die Ausführung des DHCP-Daemon beeinflussen. Sie müssen die Bedeutung jeder Aktion kennen, damit Sie das richtige Verfahren für das gewünschte Ergebnis auswählen können. Die Begriffe für die Aktionen lauten wie folgt:

- **Befehle zum Starten, Stoppen und Neustarten** wirken sich nur in der aktuellen Sitzung auf den Daemon aus. Wenn Sie den DHCP-Service z. B. stoppen, wird der Daemon beendet, aber beim Booten des Systems neu gestartet. Das Stoppen des Services wirkt sich nicht auf die DHCP-Datentabellen aus. Um den DHCP-Service vorübergehend zu starten oder zu stoppen, ohne den Service zu aktivieren bzw. zu deaktivieren, können Sie DHCP Manager oder SMF-Befehle verwenden.
- **Befehle zum Aktivieren und Deaktivieren** wirken sich in der aktuellen und in künftigen Sitzungen auf den Daemon aus. Wenn Sie den DHCP-Service deaktivieren, wird der aktuell ausgeführte Daemon beendet und beim Booten des Servers nicht neu gestartet. Sie müssen den DHCP-Daemon aktivieren, damit er beim Booten des Systems automatisch gestartet wird. DHCP-Datentabellen sind nicht betroffen. Zum Aktivieren und Deaktivieren des DHCP-Services können Sie DHCP Manager, den Befehl `dhcpconfig` oder die SMF-Befehle verwenden.
- Der **Befehl zum Dekonfigurieren** fährt den Daemon herunter, verhindert, dass der Daemon beim Booten des Systems neu gestartet wird und ermöglicht Ihnen das Löschen der DHCP-Datentabellen. Zum Dekonfigurieren des DHCP-Services können Sie DHCP Manager oder den Befehl `dhcpconfig` verwenden. Die Dekonfiguration ist in Kapitel 14, „Konfiguration des DHCP-Services (Aufgaben)" beschrieben.

Hinweis – Falls ein Server über mehrere Netzwerkschnittstellen verfügt und Sie die DHCP-Services nicht in allen Netzwerken bereitstellen möchten, lesen Sie „Angabe der Netzwerkschnittstellen für die DHCP-Verwaltung" auf Seite 389.

Mit dem folgenden Verfahren können Sie den DHCP-Service starten, stoppen, aktivieren und deaktivieren.

▼ So starten und stoppen Sie den DHCP-Service (DHCP Manager)

1. **Melden Sie sich als Superuser beim DHCP-Serversystem an.**

2. **Starten Sie DHCP Manager.**

```
# /usr/sadm/admin/bin/dhcpmgr &
```

3. **Führen Sie einen der folgenden Schritte aus:**

   - **Wählen Sie „Start" im Menü „Service", um den DHCP-Service zu starten.**
   - **Wählen Sie „Stopp" im Menü „Service", um den DHCP-Service zu stoppen.**

     Der DHCP-Daemon wird gestoppt, bis er neu gestartet oder das System gebootet wird.
   - **Wählen Sie „Neu starten" im Menü „Service", um dem DHCP-Service zu stoppen und unmittelbar neu zu starten.**

▼ So aktivieren und deaktivieren Sie den DHCP-Service (DHCP Manager)

● **Führen Sie in DHCP Manager einen der folgenden Schritte aus:**

   - **Wählen Sie „Aktivieren" im Menü „Service", um den DHCP-Daemon für einen automatischen Start beim Booten des Systems zu konfigurieren.**

     Ist der DHCP-Service aktiviert, wird er unmittelbar gestartet.
   - **Wählen Sie „Deaktivieren" im Menü „Service", um zu verhindern, dass der DHCP-Daemon beim Booten des Systems automatisch gestartet wird.**

     Ist der DHCP-Service deaktiviert, wird er unmittelbar gestoppt.

So aktivieren und deaktivieren Sie den DHCP-Service (`dhcpconfig -S`)

1. **Melden Sie sich beim DHCP-Serversystem an.**

2. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

3. **Wählen Sie eine der folgenden Aktionen:**

   - **Zum Aktivieren des DHCP-Services geben Sie den folgenden Befehl ein:**

     ```
     # /usr/sbin/dhcpconfig -S -e
     ```

   - **Zum Deaktivieren des DHCP-Services geben Sie den folgenden Befehl ein:**

     ```
     # /usr/sbin/dhcpconfig -S -d
     ```

DHCP-Service und die Service Management Facility

Die Service Management Facility (SMF) ist im Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration* beschrieben. Mit dem SMF-Befehl `svcadm` können Sie den DHCP-Server aktivieren und starten bzw. deaktivieren und stoppen. Sie können die SMF-Befehle jedoch nicht zum Modifizieren der DHCP-Service-Optionen verwenden, mit denen DHCP-Tools eingerichtet werden. Insbesondere können die Service-Optionen, die in der `/etc/dhcp/dhcpsvc.conf`-Datei gespeichert sind, nicht mit dem SMF-Tools geändert werden.

In der folgenden Tabelle sind die DHCP-Befehle den entsprechenden SMF-Befehlen zugeordnet.

TABELLE 15–1 SMF-Befehle für Aufgaben am DHCP-Server

Aufgabe	DHCP-Befehl	SMF-Befehl
DHCP-Service aktivieren	`dhcpconfig -S -e`	`svcadm enable svc:/network/dhcp-server`
DHCP-Service deaktivieren	`dhcpconfig -S -d`	`svcadm disable svc:/network/dhcp-server`

TABELLE 15–1 SMF-Befehle für Aufgaben am DHCP-Server *(Fortsetzung)*

Aufgabe	DHCP-Befehl	SMF-Befehl
DHCP-Service nur für die aktuelle Sitzung starten	Keinen	`svcadm enable -t svc:/network/dhcp-server`
DHCP-Service nur für die aktuelle Sitzung stoppen	Keinen	`svcadm disable -t svc:/network/dhcp-server`
DHCP-Service neustarten	`dhcpconfig -S -r`	`svcadm restart svc:/network/dhcp-server`

Bearbeiten von DHCP-Service-Optionen (Übersicht der Schritte)

Sie können die Werte bestimmter zusätzlicher Optionen des DHCP-Services ändern, die während der Erstkonfiguration mit DHCP Manager nicht angezeigt wurden. Zum Ändern der Service-Optionen können Sie das Dialogfeld „Service-Optionen ändern" in DHCP Manager verwenden. Oder Sie geben die Optionen mit dem Befehl `dhcpconfig` an.

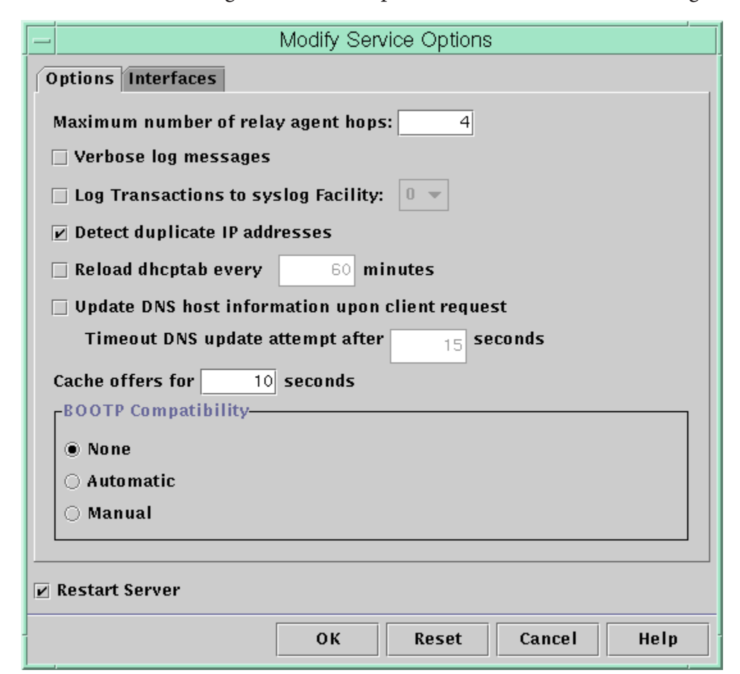
In der folgenden Tabelle werden Aufgaben zum Ändern von DHCP-Service-Optionen beschrieben. Außerdem enthält die Tabelle Links zu den Verfahren, in denen die Ausführung der Aufgaben beschrieben wird.

Aufgabe	Beschreibung	Siehe
Ändern der Protokollierungsoptionen.	Aktivieren oder deaktivieren Sie die Protokollierung, und wählen Sie die für die Protokollierung der DHCP-Transaktionen zu verwendende `syslog`-Einrichtung.	„So erzeugen Sie ausführliche DHCP-Protokollmeldungen (DHCP Manager)" auf Seite 379 „So erzeugen Sie ausführliche DHCP-Protokollmeldungen (Befehlszeile)" auf Seite 379 „So aktivieren und deaktivieren Sie die DHCP-Transaktionsprotokollierung (DHCP Manager)" auf Seite 380 „So aktivieren und deaktivieren Sie die DHCP-Transaktionsprotokollierung (Befehlszeile)" auf Seite 381 „So zeichnen Sie die DHCP-Transaktionen in einer separaten `syslog`-Datei auf" auf Seite 381

Aufgabe	Beschreibung	Siehe
Ändern der DNS-Aktualisierungsoptionen.	Aktivieren oder deaktivieren Sie die Funktion des Servers zum dynamischen Hinzufügen von DNS-Einträgen, die Clients einen Hostnamen bereitstellen. Legen Sie fest, wie lange der Server maximal versuchen soll, DNS zu aktualisieren.	„So aktivieren Sie die dynamische DNS-Aktualisierung für DHCP-Clients“ auf Seite 383
Aktivieren oder deaktivieren der Erkennung doppelt vorhandener IP-Adressen.	Aktivieren oder deaktivieren Sie die Funktion des Servers, festzustellen, ob eine IP-Adresse bereits verwendet wird, bevor sie einem Client angeboten wird.	„So passen Sie die Optionen für die DHCP-Leistung an (DHCP Manager)“ auf Seite 387 „So passen Sie die Optionen für die DHCP-Leistung an (Befehlszeile)“ auf Seite 387
Ändern der Optionen zum Einlesen der Konfigurationsinformationen durch den DHCP-Server.	Aktivieren oder deaktivieren Sie das automatische Einlesen der `dhcptab`-Tabelle in festgelegten Intervallen, oder ändern Sie das Intervall.	„So passen Sie die Optionen für die DHCP-Leistung an (DHCP Manager)“ auf Seite 387 „So passen Sie die Optionen für die DHCP-Leistung an (Befehlszeile)“ auf Seite 387
Ändern der Anzahl der Relay-Agent-Hops.	Erhöhen oder verringern Sie die Anzahl der Netzwerke, die eine Anforderung durchlaufen kann, bevor sie vom DHCP-Daemon abgeworfen wird.	„So passen Sie die Optionen für die DHCP-Leistung an (DHCP Manager)“ auf Seite 387 „So passen Sie die Optionen für die DHCP-Leistung an (Befehlszeile)“ auf Seite 387
Ändern der Zeit, über die das Angebot einer IP-Adresse zwischengespeichert wird.	Erhöhen oder verringern Sie die Zeit in Sekunden, die der DHCP-Service für eine angebotene IP-Adresse reserviert, bevor die Adresse einem anderen Client angeboten wird.	„So passen Sie die Optionen für die DHCP-Leistung an (DHCP Manager)“ auf Seite 387 „So passen Sie die Optionen für die DHCP-Leistung an (Befehlszeile)“ auf Seite 387

Die folgende Abbildung zeigt das Dialogfeld „Service-Optionen ändern“ in DHCP Manager.

ABBILDUNG 15–3 Dialogfeld „Service-Optionen ändern" in DHCP Manager



Ändern der DHCP-Protokollierungsoptionen

Der DHCP-Service kann DHCP-Servicemeldungen und DHCP-Transaktionen im `syslog` aufzeichnen. Weitere Informationen zum `syslog` finden Sie in den Manpages `syslogd(1M)` und `syslog.conf(4)`.

DHCP-Servicemeldungen, die im `syslog` aufgezeichnet werden, umfassen Folgendes:

- Fehlermeldungen, die Sie über Zustände informieren, die verhindern, dass der DHCP-Service eine Anforderung von Ihnen oder einem Client ausführen kann.
- Warnungen und Hinweise, die Sie über abnormale Zustände informieren, jedoch nicht verhindern, dass der DHCP-Service eine Anforderung ausführt.

Mit der verbose-Option für den DHCP-Daemon können Sie die Menge der angezeigten Informationen erhöhen. Die ausführliche Anzeige hilft Ihnen bei der Behebung von DHCP-Problemen. Lesen Sie dazu „So erzeugen Sie ausführliche DHCP-Protokollmeldungen (DHCP Manager)" auf Seite 379.

Eine weitere nützliche Fehlerbehebungstechnik ist die Protokollierung von Transaktionen. Transaktionen enthalten Informationen über jeden Datenaustausch zwischen DHCP-Server oder BOOTP-Relay und Clients. DHCP-Transaktionen umfassen die folgenden Meldungstypen:

- ASSIGN – IP-Adresszuweisung
- ACK – Der Server bestätigt, dass der Client die angebotene IP-Adresse akzeptiert hat und sendet Konfigurationsparameter
- EXTEND – Leasing-Verlängerung
- RELEASE – IP-Adressfreigabe
- DECLINE – Der Client verweigert die Adresszuweisung
- INFORM – Der Client fordert Netzwerkkonfigurationsparameter, aber keine IP-Adresse an
- NAK – Der Server hat die Anforderung eines Clients zum Verwenden einer zuvor verwendeten IP-Adresse nicht bestätigt
- ICMP_ECHO – Der Server hat erkannt, dass eine potentielle IP-Adresse bereits von einem anderen Host verwendet wird

BOOTP-Relay-Transaktionen umfassen die folgenden Meldungstypen:

- RELAY-CLNT – Die Meldung wird vom DHCP-Client an einen DHCP-Server weitergeleitet
- RELAY–SRVR – Die Meldung wird vom DHCP-Server an den DHCP-Client weitergeleitet

Die Protokollierung von DHCP-Transaktionen ist standardmäßig deaktiviert. Nach der Aktivierung verwendet die Protokollierung von DHCP-Transaktionen standardmäßig die Funktion `local0` in `syslog.` DHCP-Transaktionsmeldungen werden mit dem `syslog`-Schweregrad *notice* erzeugt. Dieser Schweregrad sorgt dafür, dass DHCP-Transaktionen in der Datei aufgezeichnet werden, in der auch andere Systemhinweise protokolliert werden. Da die Funktion `local` verwendet wird, können die DHCP-Transaktionsmeldungen separat von anderen Hinweisen aufgezeichnet werden. Um die Transaktionsmeldungen separat aufzuzeichnen, müssen Sie eine separate Protokolldatei in der `syslog.conf`-Datei angeben. Weitere Informationen zur `syslog.conf`-Datei finden Sie in der Manpage `syslog.conf`(4).

Sie können die Transaktionsprotokollierung deaktivieren oder aktivieren, und Sie können eine andere `syslog`-Funktion (von `local0` bis `local7`) angeben. Dies wird unter „So aktivieren und deaktivieren Sie die DHCP-Transaktionsprotokollierung (DHCP Manager)“ auf Seite 380 beschrieben. Außerdem können Sie in der `syslog.conf`-Datei des Serversystems `syslogd` anweisen, die DHCP-Transaktionsmeldungen in einer separaten Datei zu speichern. Weitere Informationen finden Sie unter „So zeichnen Sie die DHCP-Transaktionen in einer separaten `syslog`-Datei auf“ auf Seite 381.

▼ So erzeugen Sie ausführliche DHCP-Protokollmeldungen (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Option „Ändern" im Menü „Service" aus.**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

   Das Dialogfeld „Service-Optionen ändern" wird geöffnet und zeigt die Registerkarte „Optionen". Siehe dazu Abbildung 15–3.

2. **Wählen Sie „Ausführliche Protokollmeldungen".**

3. **Wählen Sie „Server erneut starten".**

   Die Option „Server erneut starten" wird am unteren Rand des Dialogfeld angezeigt.

4. **Klicken Sie auf „OK".**

   Der Daemon wird während dieser Sitzung und in allen nachfolgenden Sitzungen im ausführlichen Modus ausgeführt, bis Sie diese Option zurücksetzen. Der ausführliche Modus kann die Daemon-Effizienz reduzieren, da mehr Zeit erforderlich ist, die Meldungen anzuzeigen.

▼ So erzeugen Sie ausführliche DHCP-Protokollmeldungen (Befehlszeile)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Geben Sie den folgenden Befehl ein, um den ausführlichen Modus aufzurufen:**

   ```
   # /usr/sbin/dhcpconfig -P VERBOSE=true
   ```

   Wenn der DHCP-Server das nächste Mal gestartet wird, wird er im ausführlichen Modus ausgeführt, bis Sie diesen Modus explizit deaktivieren.

   Sie deaktivieren den ausführlichen Modus mit dem folgenden Befehl:

   ```
   # /usr/sbin/dhcpconfig -P VERBOSE=
   ```

Mit diesem Befehl wird dem Schlüsselwort `VERBOSE` kein Wert zugewiesen, wodurch das Schlüsselwort aus der Server-Konfigurationsdatei entfernt wird.

Der ausführliche Modus kann die Daemon-Effizienz reduzieren, da mehr Zeit erforderlich ist, die Meldungen anzuzeigen.

▼ So aktivieren und deaktivieren Sie die DHCP-Transaktionsprotokollierung (DHCP Manager)

Mit diesem Verfahren wird die Transaktionsprotokollierung für alle nachfolgenden DHCP-Serversitzungen aktiviert bzw. deaktiviert.

1. **Wählen Sie in DHCP Manager die Option „Ändern" im Menü „Service" aus.**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie „Transaktionen in syslog protokollieren".**

   Heben Sie die Auswahl dieser Option auf, um die Transaktionsprotokollierung zu deaktivieren.

3. **(Optional) Wählen Sie eine local-Einrichtung von 0 bis 7, die zur Protokollierung von DHCP-Transaktionen verwendet werden soll.**

   Standardmäßig werden DHCP-Transaktionen an dem Speicherort protokolliert, an dem auch die Systemhinweise gespeichert werden. Dies hängt von der Konfiguration von `syslogd` ab. Wenn Sie die DHCP-Transaktionen getrennt von anderen Systemhinweisen in einer Datei speichern möchten, lesen Sie „So zeichnen Sie die DHCP-Transaktionen in einer separaten `syslog`-Datei auf" auf Seite 381.

   Bei aktivierter Transaktionsprotokollierung können die Meldungsdateien schnell sehr groß werden.

4. **Wählen Sie „Server erneut starten".**

5. **Klicken Sie auf „OK".**

   Der Daemon protokolliert die Transaktionen während dieser und aller nachfolgenden Sitzungen im ausgewählten `syslog`, bis Sie die Protokollierung explizit wieder deaktivieren.

▼ So aktivieren und deaktivieren Sie die DHCP-Transaktionsprotokollierung (Befehlszeile)

1 Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.

Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2 Führen Sie einen der folgenden Schritte aus:

- **Zum Aktivieren der DHCP-Transaktionsprotokollierung geben Sie den folgenden Befehl ein:**

  ```
  # /usr/sbin/dhcpconfig -P LOGGING_FACILITY=syslog-local-facility
  ```

  syslog-local-facility ist eine Zahl im Bereich von 0 bis 7. Wenn Sie diese Option auslassen, wird 0 verwendet.

  Standardmäßig werden DHCP-Transaktionen an dem Speicherort protokolliert, an dem auch die Systemhinweise gespeichert werden. Dies hängt von der Konfiguration von `syslogd` ab. Wenn Sie die DHCP-Transaktionen getrennt von anderen Systemhinweisen in einer Datei speichern möchten, lesen Sie „So zeichnen Sie die DHCP-Transaktionen in einer separaten `syslog`-Datei auf“ auf Seite 381.

  Bei aktivierter Transaktionsprotokollierung können die Meldungsdateien schnell sehr groß werden.

- **Zum Deaktivieren der DHCP-Transaktionsprotokollierung geben Sie den folgenden Befehl ein:**

  ```
  # /usr/sbin/dhcpconfig -P LOGGING_FACILITY=
  ```

  Beachten Sie, das Sie keinen Wert für den Parameter angeben.

▼ So zeichnen Sie die DHCP-Transaktionen in einer separaten `syslog`-Datei auf

1 Melden Sie sich als Superuser beim DHCP-Serversystem an, oder nehmen Sie eine entsprechende Rolle an.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

Eine Rolle, der das DHCP Management-Profil zugewiesen ist, reicht eventuell für diese Aufgabe nicht aus. Der Rolle muss eine Berechtigung zum Bearbeiten von `syslog`-Dateien zugewiesen sein.

2 **Fügen Sie der `/etc/syslog.conf`-Datei auf dem Serversystem eine Zeile mit der folgenden Syntax hinzu:**

`local`*n*`.notice`   *path-to-logfile*

n ist die Zahl der `syslog`-Einrichtung, die Sie für die Transaktionsprotokollierung angegeben haben, und *Pfad-zur-Protokolldatei* ist der vollständige Pfad zu der Datei, in der die Transaktionen protokolliert werden.

Sie können z. B. die folgende Zeile hinzufügen:

```
local0.notice /var/log/dhcpsrvc
```

Weitere Informationen zur `syslog.conf`-Datei finden Sie in der Manpage `syslog.conf(4)`.

Aktivieren von dynamischen DNS-Aktualisierungen durch einen DHCP-Server

DNS bietet Name-zu-Adresse- und Adresse-zu-Name-Services für das Internet. Nachdem eine DNS-Zuordnung erfolgt ist, kann ein System über seinen Hostnamen oder seine IP-Adresse erreicht werden. Das System ist auch außerhalb seiner Domäne erreichbar.

Der DHCP-Service kann DNS auf zwei Arten verwenden:

- Der DHCP-Server kann den Hostnamen nachschlagen, der einer IP-Adresse zugeordnet ist, die der Server dem Client zugewiesen hat. Dann gibt der Server den Hostnamen des Clients zusammen mit anderen Konfigurationsinformationen des Clients zurück.
- Der DHCP-Server kann versuchen, im Auftrag des Clients eine DNS-Zuordnung vorzunehmen, wenn der DHCP-Server zum Aktualisieren von DNS konfiguriert ist. Der Client kann beim Anfordern des DHCP-Services seinen eigenen Hostnamen angeben. Wurde der DHCP-Server zum Aktualisieren von DNS konfiguriert, versucht er, DNS mit dem vom Client vorgeschlagenen Hostnamen zu aktualisieren. Ist die DNS-Aktualisierung erfolgreich, gibt der DHCP-Server den angeforderten Hostnamen an den Client zurück. Ist die DNS-Aktualisierung nicht erfolgreich, gibt der DHCP-Server einen anderen Hostnamen an den Client zurück.

Sie können den DHCP-Service zum Aktualisieren des DNS-Services für DHCP-Clients aktivieren, die einen eigenen Hostnamen angeben. Damit eine DNS-Aktualisierung ordnungsgemäß durchgeführt werden kann, müssen DNS-Server, DHCP-Server und DHCP-Client korrekt eingerichtet sein. Darüber hinaus darf der angeforderte Hostname von keinem anderen System in der Domäne verwendet werden.

Die DNS-Aktualisierung durch den DHCP-Server kann nur dann ausgeführt werden, wenn die folgenden Aussagen wahr sind:

- Der DNS-Server unterstützt RFC 2136.
- Die DNS-Software basiert auf BIND v8.2.2, Patch-Level 5 oder aktueller, entweder auf dem DHCP-Serversystem oder dem DNS-Serversystem.
- Der DNS-Server ist so konfiguriert, dass dynamische DNS-Aktualisierungen vom DHC IP-Server akzeptiert werden.
- Der DHCP-Server ist zum Durchführen von dynamischen DNS-Aktualisierungen konfiguriert.
- Die DNS-Unterstützung ist für das DHCP-Clientnetzwerk auf dem DHCP-Server konfiguriert.
- Der DHCP-Client ist so konfiguriert, dass er einen angeforderten Hostnamen in der DHCP-Anforderungsnachricht übermittelt.
- Der angeforderte Hostnamen entspricht einer DHCP-eigenen Adresse. Der Hostname kann auch noch keine entsprechende Adresse aufweisen.

▼ So aktivieren Sie die dynamische DNS-Aktualisierung für DHCP-Clients

---

Hinweis – Dynamische DNS-Aktualisierungen stellen ein *Sicherheitsrisiko* dar.

Standardmäßig gestattet der Oracle Solaris DNS-Daemon (`in.named`) keine dynamischen Aktualisierungen. Die Autorisierung für dynamische DNS-Aktualisierungen wird in der Konfigurationsdatei `named.conf` auf dem DNS-Serversystem erteilt. Andere Sicherheitsfunktionen sind nicht implementiert. Bevor Sie dynamische DNS-Aktualisierungen gestatten, müssen Sie die Vorteile dieser Funktion für Benutzer sorgfältig gegen die Sicherheitsrisiken abwägen.

---

1. **Melden Sie sich als Superuser an und bearbeiten Sie die Datei `/etc/named.conf` auf dem DNS-Server.**

2. **Suchen Sie in der Datei `named.conf` nach dem Abschnitt `zone` für die entsprechende Domäne.**

3. **Fügen Sie die IP-Adressen des DHCP-Servers zum Schlüsselwort `allow-update` hinzu.**

   Wenn das Schlüsselwort `allow-update` nicht vorhanden ist, müssen Sie es hinzufügen.

   Befindet sich der DHCP-Server an den Adressen `10.0.0.1` und `10.0.0.2`, so muss die Datei `named.conf` für die Zone `dhcp.domain.com` wie folgt geändert werden:

```
zone "dhcp.domain.com" in {
             type master;
```

```
                file "db.dhcp";
                allow-update { 10.0.0.1; 10.0.0.2; };
};

zone "10.IN-ADDR.ARPA" in {
                type master;
                file "db.10";
                allow-update { 10.0.0.1; 10.0.0.2; };
};
```

Beachten Sie, dass `allow-update` für beide Zonen aktiviert sein muss, damit der DHCP-Server sowohl A- als auch PTR-Datensätze auf dem DNS-Server aktualisieren kann.

4. **Starten Sie DHCP-Manager auf dem DHCP-Server.**

```
# /usr/sadm/admin/bin/dhcpmgr &
```

Ausführliche Informationen finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

5. **Wählen Sie die Option „Ändern“ im Menü „Service“ aus.**

Das Dialogfeld „Service-Optionen ändern“ wird angezeigt.

6. **Wählen Sie „DNS-Host-Informationen bei Client-Anforderung aktualisieren“.**

7. **Geben Sie in Sekunden an, wie lange auf eine Antwort vom DNS-Server gewartet werden soll, bevor eine Zeitüberschreitung eintritt, und klicken Sie auf „OK“.**

Der Standardwert von 15 Sekunden ist in der Regel ausreichend. Falls Probleme mit der Zeitüberschreitung auftreten, können Sie den Wert erhöhen.

8. **Klicken Sie auf die Registerkarte „Makros“ und stellen Sie sicher, dass die richtige DNS-Domäne angegeben ist.**

Die Option `DNSdmain` muss mit dem richtigen Domänennamen an jeden Client übergeben werden, der eine Unterstützung für die dynamische DNS-Aktualisierung erwartet. Standardmäßig wird `DNSdmain` im Servermakro angegeben, das als Konfigurationsmakro verwendet wird, das an jede IP-Adresse gebunden ist.

9. **Richten Sie den DHCP-Client so ein, dass er bei der Anforderung des DHCP-Services seinen Hostnamen angibt.**

Wenn Sie den Oracle Solaris DHCP-Client verwenden, lesen Sie „So konfigurieren Sie einen Oracle Solaris DHCPv4-Client zur Anforderung eines bestimmten Hostnamens“ auf Seite 468. Falls Ihr Client kein Oracle Solaris DHCP-Client ist, suchen Sie in der Dokumentation für Ihren DHCP-Client nach Informationen, wie ein Hostname angegeben wird.

Registrierung des Client-Hostnamen

Wenn der DHCP-Server die Hostnamen für die IP-Adressen erzeugen sollen, die Sie unter den DHCP-Service gestellt haben, kann der DHCP-Server diese Hostnamen beim NIS+, in der Datei `/etc/inet/hosts` oder bei den DNS-Namen-Services registrieren. Die Registrierung von Hostnamen kann nicht im NIS erfolgen, da NIS kein Protokoll bereitstellt, das Programmen ermöglicht, NIS-Maps zu aktualisieren oder zu füllen.

Hinweis – Der DHCP-Server kann DNS nur dann mit den erzeugten Hostnamen aktualisieren, wenn der DNS-Server und der DHCP-Server auf dem gleichen System ausgeführt werden.

Wenn ein DHCP-Client seinen Hostnamen bereitstellt und der DNS-Server so konfiguriert ist, dass dynamische Aktualisierungen von einem DHCP-Server aus möglich sind, kann der DHCP-Server das DNS im Auftrag des Clients aktualisieren. Dynamische Aktualisierungen können auch dann durchgeführt werden, wenn sich die DNS- und DHCP-Server auf unterschiedlichen Systemen befinden. Weitere Informationen zum Aktivieren dieser Funktion finden Sie unter „Aktivieren von dynamischen DNS-Aktualisierungen durch einen DHCP-Server“ auf Seite 382.

In der folgenden Tabelle ist die Registrierung von Hostnamen für DHCP-Clientsysteme bei verschiedenen Namen-Services zusammengefasst.

TABELLE 15–2 Registrierung von Client-Hostnamen bei Namen-Services

	Wer registriert Hostnamen	
Namen-Service	**DHCP-erzeugter Hostname**	**DHCP-Client-angegebener Hostname**
NIS	NIS Administrator	NIS Administrator
NIS+	DHCP-Tools	DHCP-Tools
`/etc/hosts`	DHCP-Tools	DHCP-Tools
DNS	DHCP-Tools, wenn der DNS-Server auf dem gleichen System wie der DHCP-Server ausgeführt wird	DHCP-Server, wenn dieser für dynamische DNS-Aktualisierungen konfiguriert ist
	DNS-Administrator, wenn der DNS-Server auf einem anderen System ausgeführt wird	DNS-Administrator, wenn der DHCP-Server nicht für dynamische Aktualisierungen konfiguriert ist

Oracle Solaris DHCP-Clients können bestimmte Hostnamen in DHCP-Anforderungen anfordern, wenn sie gemäß der Beschreibung unter „So konfigurieren Sie einen Oracle Solaris DHCPv4-Client zur Anforderung eines bestimmten Hostnamens“ auf Seite 468 dazu konfiguriert wurden. Ob diese Funktion auch von anderen DHCP-Clients unterstützt wird, können Sie der jeweiligen Herstellerdokumentation entnehmen.

Anpassen der Leistungsoptionen für den DHCP-Server

Sie können Optionen ändern, die sich auf die Leistung des DHCP-Servers auswirken. Diese Optionen sind in der folgenden Tabelle beschrieben.

TABELLE 15–3 Optionen, die sich auf die Leistung des DHCP-Servers auswirken

Server-Option	Beschreibung	Schlüsselwort
Höchstzahl an BOOTP-Relay-Agent-Hops	Wenn eine Anforderung mehr als die angegebene Anzahl der BOOTP-Relay-Agents überschritten hat, wird sie abgeworfen. Die standardmäßige Höchstzahl an Relay-Agent-Hops beträgt vier. Diese Zahl ist für die meisten Netzwerke ausreichend. Ein Netzwerk könnte mehr als vier Hops erfordern, wenn DHCP-Anforderungen mehrere BOOTP-Relay-Agents durchlaufen, bevor sie einen DHCP-Server erreichen.	`RELAY_HOPS=`*ganze Zahl*
Erkennung doppelt vorhandener Adressen	In der Standardeinstellung sendet der Server einen Ping-Befehl an eine IP-Adresse, bevor die Adresse einem Client angeboten wird. Trifft keine Antwort auf Ping-Befehl ein, ist sichergestellt, dass die Adresse noch nicht verwendet wird. Sie können diese Funktion deaktivieren, um die Zeit zu verkürzen, die der Server für ein Angebot benötigt. Andererseits erhöhen Sie durch das Deaktivieren dieser Funktion die Wahrscheinlichkeit von doppelt vorhandenen IP-Adressen.	`ICMP_VERIFY=TRUE/FALSE`
`dhcptab` in bestimmten Intervallen automatisch neu laden	Der Server kann so eingestellt werden, dass er die `dhcptab`-Tabelle in einem von Ihnen festgelegten Intervall (in Minuten) automatisch einliest. Wenn Ihre Netzwerkkonfigurationsinformationen nicht regelmäßig geändert werden und Sie nicht über mehrere DHCP-Server verfügen, muss die `dhcptab`-Tabelle nicht automatisch neu eingelesen werden. Darüber hinaus können Sie mit DHCP Manager eine Option einrichten, dass der Server die `dhcptab`-Tabelle automatisch neu einliest, nachdem eine Änderung an den Daten vorgenommen wurde.	`RESCAN_INTERVAL=`*min*
Cache bietet IP-Adressen über festgelegte Intervalle an	Nachdem ein Server einem Client eine IP-Adresse angeboten hat, wird das Angebot zwischengespeichert. Solange sich das Angebot im Cache-Speicher befindet, bietet der Server diese Adresse nicht noch einmal an. Sie können eine Zeit in Sekunden einstellen, wie lange ein Angebot zwischengespeichert wird. Der Standardwert beträgt 10 Sekunden. Bei langsamen Netzwerken können Sie versuchen, die Angebotsdauer zu verlängern.	`OFFER_CACHE_TIMEOUT=`*sek*

In den folgenden Verfahren wird beschrieben, wie diese Optionen geändert werden.

▼ So passen Sie die Optionen für die DHCP-Leistung an (DHCP Manager)

1 Wählen Sie in DHCP Manager die Option „Ändern" im Menü „Service" aus.

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2 Ändern Sie die gewünschten Optionen.

Weitere Informationen zu den Optionen finden Sie in Tabelle 15–3.

3 Wählen Sie „Server erneut starten".

4 Klicken Sie auf „OK".

▼ So passen Sie die Optionen für die DHCP-Leistung an (Befehlszeile)

Änderungen an den Optionen werden erst nach einem Neustart des DHCP-Servers übernommen.

1 Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.

Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Ändern Sie eine oder mehrere der folgenden Leistungsoptionen:

```
# /usr/sbin/dhcpconfig -P keyword=value,keyword=value...
```

Schlüsselwort=*Wert* kann eines der folgenden Schlüsselwörter sein:

`RELAY_HOPS`=*ganze Zahl*	Legt die Höchstzahl an Relay-Agent-Hops fest, die ein DHCP- oder BOOTP-Datagramm durchführen kann, bevor es vom Daemon abgeworfen wird.
`ICMP_VERIFY=TRUE/FALSE`	Aktiviert oder deaktiviert die automatische Erkennung doppelt vorhandener IP-Adressen. Dieses Schlüsselwort sollte nicht auf `FALSE` gesetzt werden.

`RESCAN_INTERVAL=`*Minuten*	Legt ein Intervall in Minuten fest, in dem der DHCP-Server die Informationen der `dhcptab`-Tabelle neu einliest.
`OFFER_CACHE_TIMEOUT=`*Sekunden*	Legt die Zeit in Sekunden fest, die der DHCP-Server Angebote zwischenspeichern soll, die zur Erfassung von DHCP-Clients erweitert wurden. Die Standardeinstellung beträgt 10 Sekunden.

Beispiel 15–1 Einrichten der DHCP-Leistungsoptionen

Das Folgende ist ein Beispiel, wie alle Befehlsoptionen angegeben werden können.

```
# dhcpconfig -P RELAY_HOPS=2,ICMP_VERIFY=TRUE,\
RESCAN_INTERVAL=30,OFFER_CACHE_TIMEOUT=20
```

Hinzufügen, Modifizieren und Löschen von DHCP-Netzwerken (Übersicht der Schritte)

Wenn Sie einen DHCP-Server konfigurieren, müssen Sie auch mindestens ein Netzwerk konfigurieren, um den DHCP-Service nutzen zu können. Weitere Netzwerke können jederzeit hinzugefügt werden.

In der folgenden Tabelle sind zusätzlich Aufgaben aufgeführt, die Sie beim Arbeiten mit DHCP-Netzwerken ausführen können, nachdem diese erstmals konfiguriert wurden. Die Tabelle enthält Links zu den Verfahren, in denen die Ausführung der Aufgaben beschrieben wird.

Aufgabe	Beschreibung	Siehe
Aktivieren oder Deaktivieren des DHCP-Service auf den Server-Netzwerkschnittstellen	Das Standardverhalten ist das Überwachen aller Netzwerkschnittstellen auf DHCP-Anforderungen. Wenn Sie nicht möchten, dass alle Schnittstellen DHCP-Anforderungen akzeptieren, können Sie bestimmte Schnittstelle aus der Liste der überwachten Schnittstellen entfernen.	„So geben Sie die Netzwerkschnittstellen an, die unter die DHCP-Verwaltung gestellt werden sollen (DHCP Manager)“ auf Seite 390
Hinzufügen eines neuen Netzwerks zum DHCP-Service.	Stellen Sie ein Netzwerk unter die DHCP-Verwaltung, um die IP-Adressen in diesem Netzwerk zu verwalten.	„So fügen Sie ein DHCP-Netzwerk hinzu (DHCP Manager)“ auf Seite 392 „So fügen Sie ein DHCP-Netzwerk hinzu (`dhcpconfig`)“ auf Seite 393

Aufgabe	Beschreibung	Siehe
Ändern der Parameter eines DHCP-verwalteten Netzwerks.	Ändern Sie die Informationen, die an Clients eines bestimmten Netzwerks übergeben laden.	„So ändern Sie die Konfiguration eines DHCP-Netzwerks (DHCP Manager)“ auf Seite 395 „So ändern Sie die Konfiguration eines DHCP-Netzwerks (`dhtadm`)“ auf Seite 396
Löschen eines Netzwerks vom DHCP-Service.	Entfernen Sie ein Netzwerk, so dass die IP-Adressen in diesem Netzwerk nicht mehr von DHCP verwaltet werden.	„So löschen Sie ein DHCP-Netzwerk (DHCP Manager)“ auf Seite 398 „So löschen Sie ein DHCP-Netzwerk (`pntadm`)“ auf Seite 398

Angabe der Netzwerkschnittstellen für die DHCP-Verwaltung

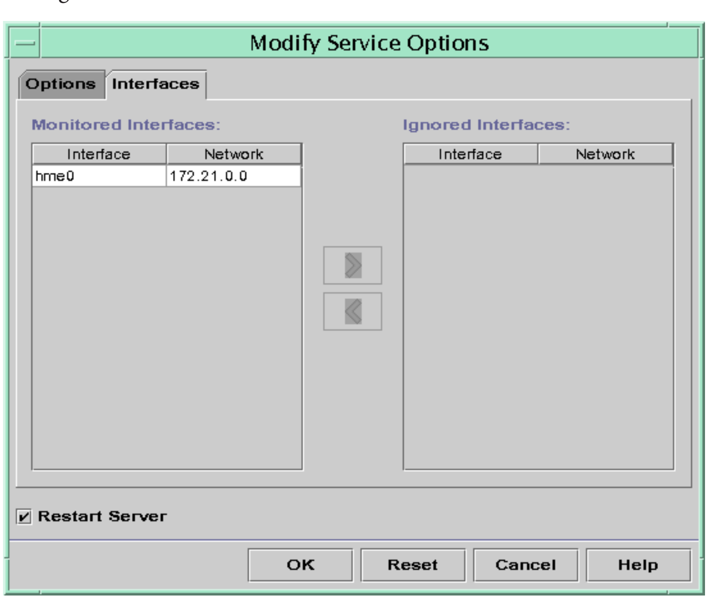
Standardmäßig wird der DHCP-Server sowohl von `dhcpconfig` als auch dem Konfigurationsassistenten von DHCP Manager so konfiguriert, dass alle Netzwerkschnittstellen eines Serversystems überwacht werden. Wenn Sie eine neue Netzwerkschnittstelle zum Serversystem hinzufügen, überwacht der DHCP-Server die neue Schnittstelle automatisch, wenn Sie das System booten. Sie können auch zusätzliche Netzwerke hinzufügen, die über die Netzwerkschnittstelle überwacht werden.

Außerdem ist es möglich, die zu überwachenden Netzwerkschnittstellen und die zu ignorierenden Schnittstellen anzugeben. Sie können eine Schnittstelle ignorieren, wenn in diesem Netzwerk keine DHCP-Services angeboten werden sollen.

Wenn Sie angeben, dass eine Schnittstelle ignoriert werden soll, und dann eine neue Schnittstelle installieren, so ignoriert der DHCP-Server diese neue Schnittstelle. Sie müssen die neue Schnittstelle der Liste der überwachten Schnittstellen auf dem Server hinzufügen. Schnittstellen können Sie mit DHCP Manager oder dem Dienstprogramm `dhcpconfig` angeben.

Dieser Abschnitt enthält Verfahren, mit denen Sie festlegen können, welche Netzwerkschnittstellen DHCP ignorieren oder überwachen soll. Die DHCP Manager-Verfahren nutzen die Registerkarte „Schnittstellen“ im Dialogfeld „Service-Optionen ändern“, das in der folgenden Abbildung gezeigt wird.

ABBILDUNG 15–4 Registerkarte „Schnittstellen“ im Dialogfeld „Service-Optionen ändern“ in DHCP Manager



▼ So geben Sie die Netzwerkschnittstellen an, die unter die DHCP-Verwaltung gestellt werden sollen (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Option „Ändern“ im Menü „Service“ aus.**

   Das Dialogfeld „Service-Optionen ändern“ wird angezeigt.

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

2. **Wählen Sie die Registerkarte „Schnittstellen“.**

3. **Wählen Sie die entsprechenden Netzwerkschnittstelle.**

4. **Klicken Sie auf die Pfeilschaltfläche, um die Schnittstelle der gewünschten Liste hinzuzufügen.**

   Um beispielsweise eine Schnittstelle zu ignorieren, wählen Sie die Schnittstelle in der Liste „Überwachte Schnittstellen“ aus und klicken dann auf den Rechtspfeil. Daraufhin wird die Schnittstelle der Liste „Ignorierte Schnittstellen“ hinzugefügt.

5. **Wählen Sie „Server erneut starten“ und klicken Sie auf „OK“.**

   Die von Ihnen vorgenommenen Änderungen werden auch nach einem Neustart beibehalten.

▼ So geben Sie die Netzwerkschnittstellen an, die unter die DHCP-Verwaltung gestellt werden sollen (`dhcpconfig`)

1 Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.

Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2 Geben Sie den folgenden Befehl auf dem DHCP-Serversystem ein:

 # /usr/sbin/dhcpconfig -P INTERFACES=*int,int,...*

Schn, Schn,... ist eine Liste der zu überwachenden Schnittstellen. Die Schnittstellennamen müssen durch Kommata voneinander getrennt werden.

Beispielsweise geben Sie zur Überwachung der Schnittstellen `ge0` und `ge1` den folgenden Befehl ein:

```
#/usr/sbin/dhcpconfig -P INTERFACES=ge0,ge1
```

Schnittstellen, die ignoriert werden sollen, lassen Sie in der `dhcpconfig`-Befehlszeile einfach weg.

Die von Ihnen mit diesem Befehl vorgenommenen Änderungen werden auch nach einem Neustart beibehalten.

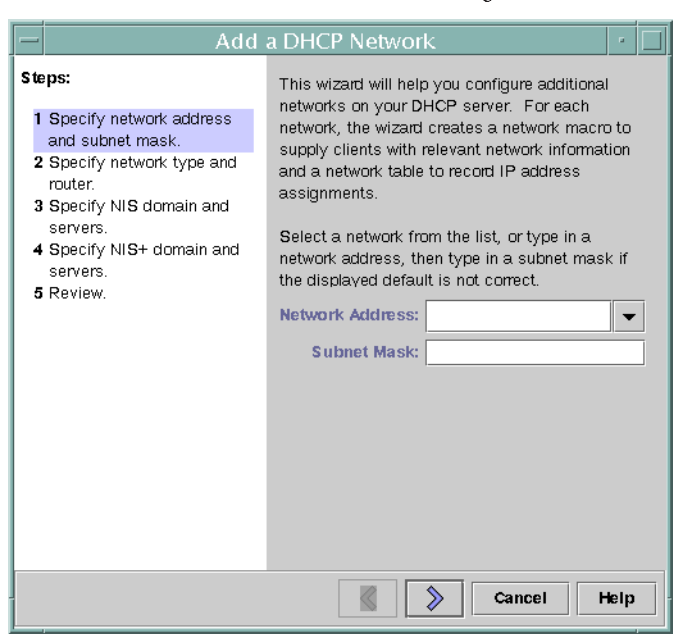
Hinzufügen von DHCP-Netzwerken

Wenn Sie DHCP Manager zur Konfiguration des Servers verwenden, wird am dabei auch das erste Netzwerk konfiguriert. Das erste Netzwerk ist in der Regel das lokale Netzwerk, mit dem die primäre Schnittstelle des Serversystems verbunden ist. Wenn Sie zusätzliche Netzwerke konfigurieren möchten, verwenden Sie den DHCP-Netzwerkassistenten in DHCP Manager.

Wenn Sie den Befehl `dhcpconfig -D` zur Konfiguration des Servers verwenden, müssen Sie alle Netzwerke, die den DHCP-Service verwenden sollen, separat konfigurieren. Weitere Informationen finden Sie unter „So fügen Sie ein DHCP-Netzwerk hinzu (`dhcpconfig`)“ auf Seite 393.

Die folgende Abbildung zeigt das erste Dialogfeld des DHCP-Netzwerkassistenten in DHCP Manager.

ABBILDUNG 15–5 Netzwerkassistent in DHCP Manager



Bei der Konfiguration eines neuen Netzwerks erstellt DHCP Manager die folgenden Komponenten:

- Eine Netzwerktabelle im Datenspeicher. Das neue Netzwerk wird in der Liste „Netzwerke“ auf der Registerkarte „Adressen“ im DHCP Manager angezeigt.
- Ein Netzwerkmakro, das die von den in diesem Netzwerk befindlichen Clients benötigten Informationen enthält. Der Name des Netzwerkmakros entspricht der IP-Adresse des Netzwerks. Das Netzwerkmakro wird der Tabelle `dhcptab` im Datenspeicher hinzugefügt.

▼ So fügen Sie ein DHCP-Netzwerk hinzu (DHCP Manager)

1 Klicken Sie in DHCP Manager auf die Registerkarte „Adressen“.

Auf dieser Registerkarte sind alle Netzwerke aufgeführt, die bereits für den DHCP-Service konfiguriert wurden.

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

2 **Wählen Sie „Netzwerkassistent" im Menü „Bearbeiten" aus.**

3 **Wählen Sie Optionen, oder geben Sie die angeforderten Informationen ein. Die anzugebenden Informationen basieren auf den Entscheidungen, die Sie während der Planungsphase getroffen haben.**

Die Planung ist unter „Planung einer DHCP-Konfiguration für remote Netzwerke" auf Seite 351 beschrieben.

Falls Sie die Probleme beim Arbeiten mit den Assistenten haben, klicken Sie im Fenster des Assistenten auf „Hilfe". Die Onlinehilfe für den DHCP-Netzwerkassistenten wird in Ihrem Webbrowser angezeigt.

4 **Klicken Sie auf „Fertig stellen", um die Netzwerkkonfiguration abzuschließen, nachdem Sie alle erforderlichen Informationen eingegeben haben.**

Der Netzwerkassistent erstellt eine leere Netzwerktabelle, die im linken Bereich des Fensters angezeigt wird.

Darüber hinaus erstellt der Netzwerkassistent ein Netzwerkmakro, dessen Name der IP-Adresse des Netzwerks entspricht.

5 **(Optional) Wählen Sie die Registerkarte „Makros" und klicken Sie dann auf das Netzwerkmakro, um den Inhalt des Makros anzuzeigen.**

So können Sie prüfen, ob die von Ihnen im Assistenten angegebenen Informationen als Werte für Optionen in das Netzwerkmakro eingetragen wurden.

Siehe auch Bevor die IP-Adressen des Netzwerks mit DHCP verwaltet werden können, müssen Sie Adressen für das Netzwerk hinzufügen. Weitere Informationen finden Sie unter „Hinzufügen von IP-Adressen zum DHCP-Service" auf Seite 406.

Auch wenn Sie die Netzwerktabelle leer lassen, kann der DHCP-Server Konfigurationsinformationen für die Clients bereitstellen. Weitere Informationen finden Sie unter „Einrichten von DHCP-Clients ausschließlich zum Empfang von Informationen (Übersicht der Schritte)" auf Seite 442.

▼ So fügen Sie ein DHCP-Netzwerk hinzu (`dhcpconfig`)

1 **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Geben Sie den folgenden Befehl auf dem DHCP-Serversystem ein:

```
# /usr/sbin/dhcpconfig -N network-address
```

Netzwerkadresse ist die IP-Adresse des Netzwerks, das Sie dem DHCP-Service hinzufügen möchten. Informationen zu den Unteroptionen, die Sie mit der Option `-N` verwenden können, finden Sie in der Manpage `dhcpconfig`(1M).

Wenn Sie keine Unteroptionen verwenden, greift `dhcpconfig` auf die Netzwerkdateien zurück, um Informationen über das Netzwerk einzuholen.

Siehe auch Bevor die IP-Adressen des Netzwerks mit DHCP verwaltet werden können, müssen Sie Adressen für das Netzwerk hinzufügen. Weitere Informationen finden Sie unter „Hinzufügen von IP-Adressen zum DHCP-Service“ auf Seite 406.

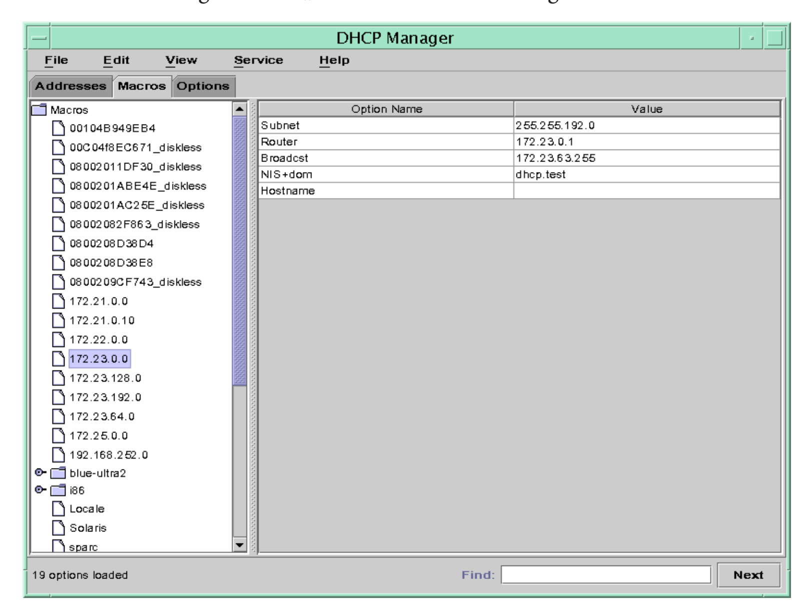
Auch wenn Sie die Netzwerktabelle leer lassen, kann der DHCP-Server Konfigurationsinformationen für die Clients bereitstellen. Weitere Informationen finden Sie unter „Einrichten von DHCP-Clients ausschließlich zum Empfang von Informationen (Übersicht der Schritte)“ auf Seite 442.

Ändern der DHCP-Netzwerkkonfigurationen

Auch nachdem Sie ein Netzwerk zum DHCP-Service hinzugefügt haben, können Sie die ursprünglich von Ihnen angegebenen Konfigurationsinformationen ändern. Die Konfigurationsinformationen sind in dem Netzwerkmakro gespeichert, das zur Übergabe von Informationen an Clients im Netzwerk verwendet wird. Zum Ändern der Netzwerkkonfiguration müssen Sie das Netzwerkmakro bearbeiten.

Die folgende Abbildung zeigt die Registerkarte „Makros“ in DHCP Manager.

ABBILDUNG 15–6 Registerkarte „Makros“ in DHCP Manager



So ändern Sie die Konfiguration eines DHCP-Netzwerks (DHCP Manager)

1 Wählen Sie in DHCP Manager die Registerkarte „Makros“.

Alle Makros, die für diesen DHCP-Server definiert wurden, werden im linken Bereich des Fensters aufgeführt.

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

2 Wählen Sie das Netzwerkmakro, dessen Name der Netzwerkkonfiguration entspricht, die Sie ändern möchten.

Der Name des Netzwerkmakros ist die IP-Adresse des Netzwerks.

3 Wählen Sie „Eigenschaften“ im Menü „Bearbeiten“ aus.

Das Dialogfeld „Eigenschaften für Makro“ zeigt eine Tabelle der Optionen an, die im Makro enthalten sind.

4 Wählen Sie die Option aus, die Sie ändern möchten.

Der Optionsname und der zugehörige Wert werden in Textfeldern im oberen Bereich des Dialogfelds angezeigt.

5. **(Optional) Ändern Sie den Optionsnamen oder klicken Sie auf die Schaltfläche „Auswählen", um eine Liste der Optionsnamen anzuzeigen.**

   Das Dialogfeld „Option wählen" zeigt eine Liste aller DHCP-Standardoptionen zusammen mit einer Kurzbeschreibung jeder Option an.

6. **(Optional) Wählen Sie einen Optionsnamen im Dialogfeld „Option wählen" aus und klicken Sie auf „OK".**

   Der neue Optionsname wird im Feld „Optionsname" angezeigt.

7. **Geben Sie einen neuen Wert für die Option ein und klicken Sie dann auf „Ändern".**

8. **(Optional) Sie können auch Optionen zum Netzwerkmakro hinzufügen, in dem Sie im Dialogfeld auf „Auswählen" klicken.**

   Allgemeine Informationen zum Ändern von Makros finden Sie unter „Ändern von DHCP-Makros" auf Seite 422.

9. **Wählen Sie „DHCP-Server von Änderung benachrichtigen" und klicken Sie auf „OK".**

   Diese Auswahl weist den DHCP-Server an, die `dhcptab`-Tabelle erneut einzulesen, um die darin vorgenommenen Änderungen unmittelbar nach dem Klicken auf „OK" zu übernehmen.

▼ So ändern Sie die Konfiguration eines DHCP-Netzwerks (`dhtadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Ermitteln Sie, welches Makro Informationen für alle Clients im Netzwerk enthält.**

   Der Name des Netzwerkmakros entspricht der IP-Adresse des Netzwerks.

   Wenn Sie nicht wissen, welches Makro diese Informationen enthält, können Sie mithilfe des Befehls `dhtadm -P` die `dhcptab`-Tabelle anzeigen, in der alle Makros aufgeführt sind.

3. **Geben Sie einen Befehl in der folgenden Syntax ein, um den Wert der gewünschten Option zu ändern:**

   ```
   # dhtadm -M -m macro-name -e 'symbol=value' -g
   ```

Weitere Informationen zu den dhtadm-Befehlszeilenoptionen finden Sie in der Manpage dhtadm(1M).

Beispiel 15–2 Verwenden des Befehls dhtadm zum Ändern eines DHCP-Makros

Um beispielsweise die Leasing-Zeit des Makros 10.25.62.0 zu 57600 Sekunden und die NIS-Domäne zu sem.example.com zu ändern, geben Sie die folgenden Befehle ein:

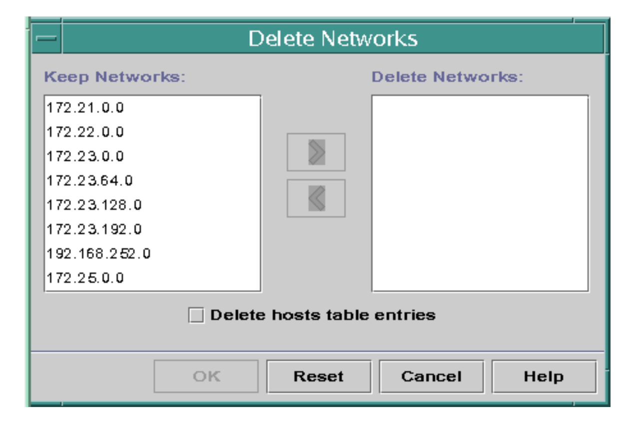
```
# dhtadm -M -m 10.25.62.0 -e 'LeaseTim=57600' -g

# dhtadm -M -m 10.25.62.0 -e 'NISdmain=sem.example.com' -g
```

Die Option -g sorgt dafür, dass der DHCP-Daemon die Tabelle dhcptab neu einliest und die darin vorgenommenen Änderungen übernimmt.

Entfernen von DHCP-Netzwerken

Mit DHCP Manager können Sie mehrere Netzwerke auf einmal entfernen. Sie können die Hosttabelleneinträge, die den DHCP-verwalteten IP-Adressen in diesen Netzwerken zugeordnet sind, automatisch mit löschen lassen. Die folgende Abbildung zeigt das Dialogfeld „Netzwerke löschen“ in DHCP Manager.

ABBILDUNG 15–7 Dialogfeld „Netzwerke löschen“ in DHCP Manager



Der Befehl pntadm erfordert, dass Sie jeden IP-Adresseintrag eines Netzwerks löschen, bevor Sie das Netzwerk löschen können. Sie können nur jeweils ein Netzwerk löschen.

▼ So löschen Sie ein DHCP-Netzwerk (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Adressen".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie „Netzwerke löschen" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Netzwerke löschen" wird angezeigt.

3. **Wählen Sie in der Liste „Netzwerke behalten" die zu löschenden Netzwerke aus.**

   Um mehrere Netzwerke auszuwählen, halten Sie während des Klickens die Strg-Taste gedrückt. Halten Sie die Umschalttaste gedrückt, um mehrere aufeinander folgende Netzwerke auszuwählen.

4. **Klicken Sie auf den Rechtspfeil, um die ausgewählten Netzwerke in die Liste „Netzwerke löschen" zu verschieben.**

5. **Wenn Sie die Hosts-Tabelleneinträge für die DHCP-Adressen dieses Netzwerks löschen möchten, aktivieren Sie das Kontrollkästchen „Hosts-Tabelleneinträge löschen".**

   Beachten Sie, dass das Löschen der Hosts-Tabelleneinträge nicht die Host-Registrierungen für diese Adressen beim DNS-Server löscht. Die Einträge werden nur beim lokalen Namen-Service gelöscht.

6. **Klicken Sie auf „OK".**

▼ So löschen Sie ein DHCP-Netzwerk (`pntadm`)

Beachten Sie, dass dieses Verfahren die IP-Adressen des Netzwerks aus der DHCP-Netzwerktabelle entfernt, bevor das Netzwerk gelöscht wird. Die Adressen werden gelöscht, um sicherzustellen, dass die Hostnamen aus der `hosts`-Datei bzw. -Datenbank gelöscht werden.

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Geben Sie einen Befehl in der folgenden Syntax ein, um eine IP-Adresse und den dazugehörigen Hostnamen aus einem Namen-Service zu löschen:**

   ```
   # pntadm -D -y IP-address
   ```

   Zum Löschen der IP-Adresse `10.25.52.1` geben Sie z. B. den folgenden Befehl ein:

   ```
   # pntadm -D -y 10.25.52.1
   ```

   Die Option `-y` gibt an, dass der Hostname gelöscht werden soll.

3. **Wiederholen Sie den Befehl `pntadm -D -y` für jede Adresse im Netzwerk.**

   Sie können auch ein Skript zum Ausführen des Befehls `pntadm` erstellen, wenn Sie viele Adressen löschen müssen.

4. **Nachdem alle Adressen gelöscht wurden, geben Sie den folgenden Befehl ein, um das Netzwerk aus dem DHCP-Service zu löschen.**

   ```
   # pntadm -R network-IP-address
   ```

   Zum Löschen des Netzwerks `10.25.52.0` geben Sie z. B. den folgenden Befehl ein:

   ```
   # pntadm -R 10.25.52.0
   ```

   Weitere Informationen zum Dienstprogramm `pntadm` finden Sie in der Manpage `pntadm`(1M).

Unterstützen von BOOTP-Clients mit dem DHCP-Service (Übersicht der Schritte)

Um BOOTP-Clients auf Ihren DHCP-Server zu unterstützen, müssen Sie Ihren DHCP-Server so einrichten, dass er BOOTP-kompatibel ist. Wenn Sie angeben möchten, welche BOOTP-Clients Ihren DHCP-Service verwenden können, müssen Sie die BOOTP-Clients in der Netzwerktabelle des DHCP-Servers registrieren. Alternativ können Sie verschiedene IP-Adressen zur automatischen Zuweisung für BOOTP-Clients reservieren.

Hinweis – BOOTP-Adressen werden permanent zugewiesen, unabhängig davon, ob Sie explizit ein permanentes Leasing der Adresse zuweisen.

In der folgenden Tabelle sind die Aufgaben aufgeführt, die Sie zur Unterstützung von BOOTP-Clients ausführen können. Die Tabelle enthält Links zu den Verfahren, in denen die Ausführung der Aufgaben beschrieben wird.

Aufgabe	Beschreibung	Siehe
Einrichten der automatischen BOOTP-Unterstützung.	Stellen Sie jedem BOOTP-Client in einem DHCP-verwalteten Netzwerk oder in einem Netzwerk, das über einen Relay-Agent mit einem DHCP-verwalteten Netzwerk verbunden ist, eine IP-Adresse bereit. Sie müssen einen Adresspool exklusiv für die Verwendung durch BOOTP-Clients reservieren. Diese Option bietet sich insbesondere dann an, wenn der Server zahlreiche BOOTP-Clients unterstützen muss.	„So richten Sie die Unterstützung für alle BOOTP-Clients ein (DHCP Manager)“ auf Seite 400
Einrichten der manuellen BOOTP-Unterstützung.	Stellen Sie nur den BOOTP-Clients, die manuell beim DHCP-Service registriert wurden, eine IP-Adresse bereit. Diese Option erfordert, dass Sie eine Client-ID an eine bestimmte IP-Adresse binden, die für BOOTP-Clients gekennzeichnet wurde. Diese Option bietet sich insbesondere bei wenigen BOOTP-Clients an, oder wenn Sie die Anzahl der BOOTP-Clients, die den DHCP-Server verwenden können, möglichst klein halten wollen.	„So richten Sie die Unterstützung von registrierten BOOTP-Clients ein (DHCP Manager)“ auf Seite 401

▼ So richten Sie die Unterstützung für alle BOOTP-Clients ein (DHCP Manager)

1 Wählen Sie in DHCP Manager die Option „Ändern“ im Menü „Service“ aus.

Das Dialogfeld „Service-Optionen ändern“ wird angezeigt.

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

2 Wählen Sie im Bereich „BOOTP-Kompatibilität“ des Dialogfelds die Option „Automatisch“.

3 Wählen Sie „Server erneut starten“ und klicken Sie auf „OK“.

4 Wählen Sie die Registerkarte „Adressen“.

5 **Wählen Sie die Adressen, die Sie für BOOTP-Clients reservieren möchten.**

Um einen Adressbereich auszuwählen, klicken Sie auf die erste Adresse, halten die Umschalttaste gedrückt und klicken dann auf die letzte Adresse. Um mehrere nicht aufeinander folgende Adressen auszuwählen, halten Sie beim Klicken auf jede Adresse die Strg-Taste gedrückt.

6 **Wählen Sie „Eigenschaften" im Menü „Bearbeiten" aus.**

Das Dialogfeld „Mehrere Adressen ändern" wird angezeigt.

7 **Wählen Sie im Bereich „BOOTP" die Option „Alle Adressen nur BOOTP-Clients zuweisen".**

Alle anderen Optionen sollten auf „Aktuelle Einstellungen beibehalten" gesetzt werden.

8 **Klicken Sie auf „OK".**

Jetzt kann jeder BOOTP-Client eine Adresse von diesem DHCP-Server beziehen.

▼ So richten Sie die Unterstützung von registrierten BOOTP-Clients ein (DHCP Manager)

1 **Wählen Sie in DHCP Manager die Option „Ändern" im Menü „Service" aus.**

Das Dialogfeld „Service-Optionen ändern" wird angezeigt.

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2 **Wählen Sie im Bereich „BOOTP-Kompatibilität" des Dialogfelds die Option „Manuell".**

3 **Wählen Sie „Server erneut starten" und klicken Sie auf „OK".**

4 **Wählen Sie die Registerkarte „Adressen".**

5 **Wählen Sie eine Adresse, die Sie einem bestimmten BOOTP-Client zuweisen möchten.**

6 **Wählen Sie „Eigenschaften" im Menü „Bearbeiten" aus.**

Das Dialogfeld „Eigenschaften für Adresse" wird angezeigt.

7 **Klicken Sie im Dialogfeld „Eigenschaften für Adresse" auf die Registerkarte „Leasing".**

8 **Geben Sie die Client-ID in das Feld „Client-ID" ein.**

Bei einem BOOTP Oracle Solaris Client in einem Ethernet-Netzwerk ist die Client-ID ein String, der von der hexadezimalen Ethernet-Adresse des Clients abgeleitet wird. Die Client-ID

beinhaltet ein Präfix, das den Address Resolution Protocol (ARP)-Typ für Ethernet (01) angibt. Bei einem BOOTP-Client mit der Ethernet-Adresse `8:0:20:94:12:1e` würde die Client-ID `0108002094121E` lauten.

Tipp – Geben Sie als Superuser auf einem Oracle Solaris Clientsystem den folgenden Befehl ein, um die Ethernet-Adresse der Schnittstelle zu beziehen:

```
# ifconfig -a
```

---

9. **Wählen Sie „Reserviert", um die IP-Adresse für diesen Client zu reservieren.**

10. **Wählen Sie „Nur BOOTP-Clients zuweisen" und klicken Sie auf „OK".**

    Auf der Registerkarte „Adressen" werden „BOOTP" im Feld „Status", und die von Ihnen angegebene Client-ID im Feld „Client-ID" angezeigt.

Arbeiten mit IP-Adressen im DHCP-Service (Übersicht der Schritte)

Mit DHCP Manager oder dem Befehl `pntadm` können Sie IP-Adressen hinzufügen, Adresseigenschaften ändern und Adressen vom DHCP-Service entfernen. Bevor Sie mit IP-Adressen arbeiten, sollten Sie Tabelle 15–4 lesen, um sich mit den Eigenschaften von IP-Adressen vertraut zu machen. Diese Tabelle enthält Informationen für die Benutzer von DHCP Manager und dem Befehl `pntadm`.

Hinweis – Tabelle 15–4 enthält Beispiele für die Verwendung von `pntadm` zur Angabe der Eigenschaften von IP-Adressen beim Hinzufügen oder Ändern von IP-Adressen. Weitere Informationen zum Befehl `pntadm(1M)` finden Sie in der Manpage `pntadm` .

In der folgenden Tabelle sind die Aufgaben aufgeführt, die Sie zum Hinzufügen, Ändern oder Entfernen von IP-Adressen ausführen müssen. Die Tabelle enthält Links zu den Verfahren, in denen die Ausführung der Aufgaben beschrieben wird.

Aufgabe	Beschreibung	Siehe
Hinzufügen einer oder mehrerer IP-Adressen zum DHCP-Service.	Fügen Sie mithilfe von DHCP Manager IP-Adressen zu Netzwerken hinzu, die bereits vom DHCP-Service verwaltet werden.	„So fügen Sie eine einzelne IP-Adresse hinzu (DHCP Manager)“ auf Seite 408 „So duplizieren Sie eine vorhandene IP-Adresse (DHCP Manager)“ auf Seite 409 „So fügen Sie mehrere IP-Adressen hinzu (DHCP Manager)“ auf Seite 409 „So fügen Sie IP-Adressen hinzu (`pntadm`)“ auf Seite 410
Ändern der Eigenschaften einer IP-Adresse.	Ändern Sie die in Tabelle 15–4 beschriebenen Eigenschaften einer IP-Adresse.	„So ändern Sie die Eigenschaften von IP-Adressen (DHCP Manager)“ auf Seite 412 „So ändern Sie die Eigenschaften von IP-Adressen (`pntadm`)“ auf Seite 412
Entfernen von IP-Adressen vom DHCP-Service.	Verhindern Sie die Verwendung der angegebenen IP-Adressen durch DHCP.	„So kennzeichnen Sie IP-Adressen als nicht verwendbar (DHCP Manager)“ auf Seite 413 „So kennzeichnen Sie IP-Adressen als nicht verwendbar (`pntadm`)“ auf Seite 414 „So löschen Sie IP-Adressen vom DHCP-Service (DHCP Manager)“ auf Seite 415 „So löschen Sie IP-Adressen vom DHCP-Service (`pntadm`)“ auf Seite 416
Zuweisen einer konstanten IP-Adresse zu einem DHCP-Client.	Richten Sie einen Client so ein, dass er jedes Mal, wenn er seine Konfiguration anfordert, die gleiche IP-Adresse erhält.	„So weisen Sie einem DHCP-Client eine konsistente IP-Adresse zu (DHCP Manager)“ auf Seite 417 „So weisen Sie einem DHCP-Client eine konsistente IP-Adresse zu (`pntadm`)“ auf Seite 418

In der folgenden Tabelle sind die Eigenschaften von IP-Adressen sowie eine Beschreibung dieser Eigenschaften aufgeführt.

TABELLE 15–4 Eigenschaften von IP-Adressen

Eigenschaft	Beschreibung	So geben Sie diese Eigenschaft im Befehl `pntadm` an
Netzwerkadresse	Die Adresse des Netzwerks, das die IP-Adresse enthält, mit der Sie arbeiten. Die Netzwerkadresse wird in der Liste „Netzwerke" auf die Registerkarte „Adressen" in DHCP Manager angezeigt.	Die Netzwerkadresse muss das letzte Argument in der Befehlszeile `pntadm` sein, die zum Erstellen, Ändern oder Löschen einer IP-Adresse verwendet wird. Um eine IP-Adresse zum Netzwerk `10.21.0.0` hinzuzufügen, geben Sie den folgenden Befehl ein: **`pntadm -A`** *IP-Adresse Optionen* **`10.21.0.0`**
IP-Adresse	Die Adresse, mit der Sie arbeiten, wenn Sie eine Adresse erstellen, ändern oder löschen. Die IP-Adresse wird in der ersten Spalte auf die Registerkarte „Adressen" in DHCP Manager angezeigt.	Die IP-Adresse muss die Optionen `-A`, `-M` und `-D` des Befehls `pntadm` begleiten. Um die IP-Adresse `10.21.5.12` zu ändern, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12`** *Optionen* **`10.21.0.0`**
Clientname	Der Hostname, der einer IP-Adresse in der hosts-Tabelle zugeordnet ist. Dieser Name kann von DHCP Manager beim Erstellen von Adressen automatisch erzeugt werden. Wenn Sie eine einzelne Adresse erstellen, können Sie den Namen angeben.	Geben Sie den Clientnamen mit der Option `-h` an. Um beispielsweise den Clientnamen `carrot12` für die Adresse `10.21.5.12` anzugeben, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -h carrot12 10.21.0.0`**
Eigentum des Servers	Der DHCP-Server, der die IP-Adresse verwaltet und auf eine Anforderung des DHCP-Clients zur Zuweisung einer IP-Adresse antwortet.	Geben Sie den Namen des betreffenden Servers mit der Option `-s` an. Um beispielsweise den Server `blue2` als Eigentümer von `10.21.5.12` anzugeben, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -s blue2 10.21.0.0`**
Konfigurationsmakro	Das Makro, das der DHCP-Server verwendet, um die Netzwerkkonfigurationsinformationen aus der `dhcptab`-Tabelle zu beziehen. Bei der Serverkonfiguration und beim Hinzufügen von Netzwerken werden automatisch mehrere Makros erstellt. Weitere Informationen zu Makros finden Sie unter „Einführung in DHCP-Makros" auf Seite 334 Beim Erstellen von Adressen wird zudem ein Servermakro erstellt. Das Servermakro wird jeder Adresse als Konfigurationsmakro zugewiesen.	Geben Sie den Makronamen mit der Option `-m` an. Um beispielsweise das Servermakro `blue2` der Adresse `10.21.5.12` zuzuweisen, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -m blue2 10.21.0.0`**

TABELLE 15–4 Eigenschaften von IP-Adressen *(Fortsetzung)*

Eigenschaft	Beschreibung	So geben Sie diese Eigenschaft im Befehl `pntadm` an
Client-ID	Ein Text-String, der innerhalb des DHCP-Services einmalig ist. Wenn die Client-ID als 00 aufgeführt ist, wird die Adresse keinem Client zugewiesen. Wenn Sie eine Client-ID beim Ändern der Eigenschaften einer IP-Adresse angeben, wird diese Adresse exklusiv an diesen Client gebunden. Die Client-ID wird vom Hersteller des DHCP-Clients festgelegt. Handelt es sich bei Ihrem Client nicht um einen Oracle Solaris DHCP-Client, suchen Sie in der Dokumentation Ihres DHCP-Clients nach weiteren Informationen. Bei Oracle Solaris DHCP-Clients wird die Client-ID von der hexadezimalen Hardwareadresse des Clients abgeleitet. Die Client-ID enthält ein Präfix, das den ARP-Code für den Netzwerktyp darstellt, z. B. 01 für Ethernet. Die Zuweisung der ARP-Codes erfolgt von der Internet Assigned Numbers Authority (IANA) im Abschnitt „ARP Parameters“ des Assigned Numbers-Standards unter `http://www.iana.com/numbers.html`. Bei einem Oracle Solaris Client mit der hexadezimalen Ethernet-Adresse `8:0:20:94:12:1e` würde die Client-ID `0108002094121E` lauten. Die Client-ID wird in DHCP Manager und `pntadm` aufgeführt, wenn ein Client derzeit eine Adresse verwendet. **Tipp:** Geben Sie als Superuser auf einem Oracle Solaris Clientsystem den folgenden Befehl ein, um die Ethernet-Adresse der Schnittstelle zu beziehen: `ifconfig -a`	Geben Sie die Client-ID mit der Option `-i` an. Um beispielsweise die Client-ID `08002094121E` zur Adresse `10.21.5.12` zuzuweisen, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -i 0108002094121E 10.21.0.0`**

TABELLE 15–4 Eigenschaften von IP-Adressen *(Fortsetzung)*

Eigenschaft	Beschreibung	So geben Sie diese Eigenschaft im Befehl `pntadm` an
Reserviert	Diese Einstellung gibt an, dass die Adresse exklusiv für den Client reserviert ist, der durch die Client-ID angegeben wird. Der DHCP-Server kann diese Adresse nicht zurückfordern. Wenn Sie diese Option wählen, müssen Sie die Adresse dem Client manuell zuweisen.	Geben Sie an, dass die Adresse reserviert ist, oder weisen Sie sie manuell mit der Option `-f` zu. Um beispielsweise anzugeben, dass die IP-Adresse `10.21.5.12` für einen Client reserviert ist, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -f MANUAL 10.21.0.0`**
Leasing-Typ oder -Richtlinie	Diese Einstellung legt fest, wie DHCP die Verwendung von IP-Adressen durch Clients verwaltet. Ein Leasing ist entweder dynamisch oder permanent. Eine ausführliche Erklärung finden Sie unter „Dynamische und permanente Leasing-Typen“ auf Seite 349.	Geben Sie die permanente Zuweisung einer Adresse mit der Option `-f` an. In der Standardeinstellung werden Adressen dynamisch geleast. Um beispielsweise anzugeben, dass die IP-Adresse `10.21.5.12` permanent geleast wird, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -f PERMANENT 10.21.0.0`**
Leasing-Ablaufdatum	Das Datum, an dem das Leasing abläuft, sofern dynamisches Leasing angegeben wurde. Das Datum muss in dem Format *mm/tt/jjjj* angegeben werden.	Geben Sie ein Leasing-Ablaufdatum mit der Option `-e` an. Um beispielsweise das Ablaufdatum 1. Januar 2006 anzugeben, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -e 01/01/2006 10.21.0.0`**
BOOTP-Einstellung	Diese Einstellung maskiert eine Adresse als reserviert für BOOTP-Clients. Weitere Informationen zur Unterstützung von BOOTP-Clients finden Sie unter „Unterstützen von BOOTP-Clients mit dem DHCP-Service (Übersicht der Schritte)“ auf Seite 399.	Reservieren Sie eine Adresse für BOOTP-Clients mit der Option `-f`. Um beispielsweise die IP-Adresse `10.21.5.12` für BOOTP-Clients zu reservieren, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -f BOOTP 10.21.0.0`**
Nicht verwendbar-Einstellung	Eine Einstellung, mit der eine Adresse markiert wird, so dass deren Zuweisung zu einem Client verhindert wird.	Markieren Sie eine Adresse mit der Option `-f` als nicht verwendbar. Um beispielsweise die IP-Adresse `10.21.5.12` als nicht verwendbar zu kennzeichnen, geben Sie den folgenden Befehl ein: **`pntadm -M 10.21.5.12 -f UNUSABLE 10.21.0.0`**

Hinzufügen von IP-Adressen zum DHCP-Service

Bevor Sie IP-Adressen hinzufügen, müssen Sie das Netzwerk, das Eigentümer der Adressen ist, zum DHCP-Service hinzufügen. Informationen zum Hinzufügen von Netzwerken finden Sie unter „Hinzufügen von DHCP-Netzwerken“ auf Seite 391.

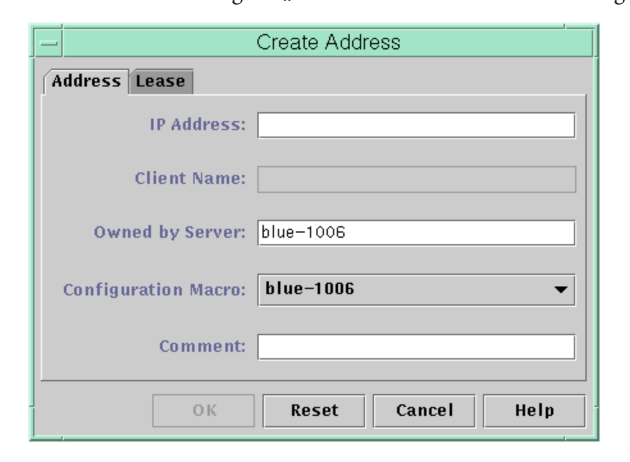
Adressen können Sie mit DHCP Manager oder dem Befehl `pntadm` hinzufügen.

Bei Netzwerken, die bereits vom DHCP-Service verwaltet werden, können Sie Adressen auf verschiedene Arten mit DHCP Manager hinzufügen:

- **Hinzufügen einer einzelnen IP-Adresse** – Stellen Sie eine neue IP-Adresse unter die DHCP-Verwaltung.
- **Duplizieren einer vorhandenen IP-Adresse** – Kopieren Sie die Eigenschaften einer vorhandenen, von DHCP verwalteten IP-Adresse, und geben Sie eine neue IP-Adresse und einen Clientnamen an.
- **Hinzufügen eines Bereichs mit mehreren IP-Adressen** – Verwenden Sie den Adressassistenten, um mehrere IP-Adressen unter die DHCP-Verwaltung zu stellen.

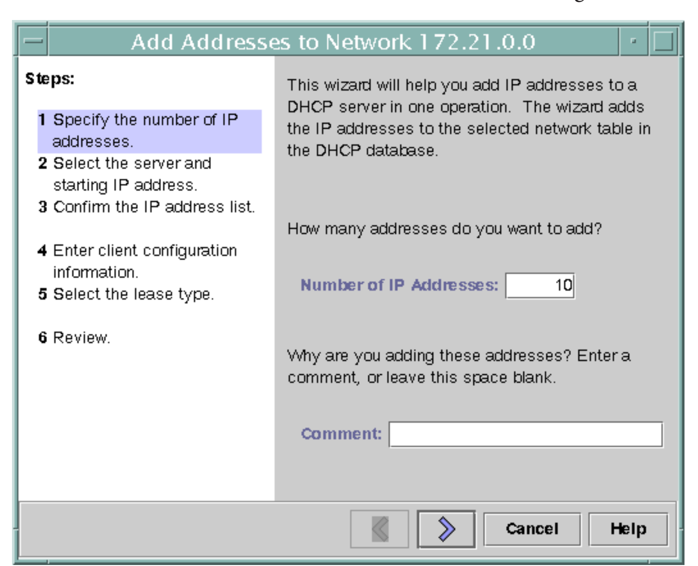
Die folgende Abbildung zeigt das Dialogfeld „Adresse erstellen". Das Dialogfeld „Adresse duplizieren" ist mit dem Dialogfeld „Adresse erstellen" identisch, mit Ausnahme der Textfelder, in denen die Werte für eine vorhandene Adresse angezeigt werden.

ABBILDUNG 15–8 Dialogfeld „Adresse erstellen" in DHCP Manager



Die folgende Abbildung zeigt das erste Dialogfeld im Assistenten „Adressen zum Netzwerk hinzufügen", über den ein Bereich von IP-Adressen hinzugefügt wird.

ABBILDUNG 15–9 Assistent „Adressen zum Netzwerk hinzufügen“ in DHCP Manager



▼ So fügen Sie eine einzelne IP-Adresse hinzu (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Adressen“.**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

2. **Wählen Sie das Netzwerk, dem die neue IP-Adresse hinzugefügt werden sollen.**

3. **Wählen Sie „Erstellen“ im Menü „Bearbeiten“ aus.**

   Das Dialogfeld „Adresse erstellen“ wird angezeigt.

4. **Wählen oder geben Sie die Werte für die Adresseinstellungen auf den Registerkarten „Adresse“ und „Leasing“ ein.**

   Klicken Sie auf die Schaltfläche „Hilfe“, um die Hilfe zu diesem Dialogfeld in Ihrem Webbrowser anzuzeigen. Ausführliche Informationen zu den Einstellungen finden Sie in Tabelle 15–4.

5. **Klicken Sie auf „OK“.**

▼ So duplizieren Sie eine vorhandene IP-Adresse (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Adressen".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie das Netzwerk, in dem sich die neue IP-Adresse befindet.**

3. **Wählen Sie die Adresse mit Eigenschaften, die Sie duplizieren möchten.**

4. **Wählen Sie „Duplizieren" im Menü „Bearbeiten" aus.**

5. **Geben Sie die neue IP-Adresse in das Feld „IP-Adressen" ein.**

6. **(Optional) Geben Sie einen neuen Clientnamen für die Adresse ein.**

   Sie müssen einen Namen eingeben, der von dem der duplizierten Adresse abweicht.

7. **(Optional) Ändern Sie gegebenenfalls Optionswerte.**

   Die meisten Optionswerte sollten jedoch gleich bleiben.

8. **Klicken Sie auf „OK".**

▼ So fügen Sie mehrere IP-Adressen hinzu (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Adressen".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie das Netzwerk, dem die neuen IP-Adressen hinzugefügt werden sollen.**

3. **Wählen Sie „Adressassistent" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Adressen zum Netzwerk hinzufügen" fordert Sie auf, Werte für die Eigenschaften der IP-Adresse einzugeben. Weitere Informationen zu den Eigenschaften finden Sie in Tabelle 15–4 oder klicken Sie im Dialogfeld auf die Schaltfläche „Hilfe". „Entscheidungen bei der Verwaltung von IP-Adressen (Übersicht der Schritte)" auf Seite 346 enthält weitere, ausführliche Informationen.

4. **Wenn die Eingaben in einem Fenster abgeschlossen sind, klicken Sie auf den Rechtspfeil und im letzten Fenster auf „Fertig stellen".**

   Die Registerkarte „Adressen" wird mit den neuen Adressen aktualisiert.

▼ So fügen Sie IP-Adressen hinzu (`pntadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Fügen Sie IP-Adressen hinzu, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

   `#` **`pntadm -A`** *ip-address options network-address*

   Eine Liste der Optionen, die Sie mit dem Befehl `pntadm`(1M) verwenden können, finden Sie in der Manpage `pntadm -A`. Darüber hinaus sind in Tabelle 15–4 einige Beispiele für `pntadm`-Befehle aufgeführt, in denen Optionen angegeben sind.

Hinweis – Sie können ein Skript schreiben, um mehrere Adressen mit dem Befehl `pntadm` hinzuzufügen. Ein Beispiel finden Sie in Beispiel 18–1.

Ändern von IP-Adressen im DHCP-Service

Mit DHCP Manager oder dem Befehl `pntadm -M` können Sie beliebige der in Tabelle 15–4 aufgeführten Adresseigenschaften ändern. Weitere Informationen zum Befehl `pntadm`(1M) finden Sie in der Manpage `pntadm -M`.

Die folgende Abbildung zeigt das Dialogfeld „Eigenschaften für Adresse", in dem Sie die Eigenschaften von IP-Adressen ändern können.

ABBILDUNG 15–10 Dialogfeld „Eigenschaften für Adresse" in DHCP Manager

Address Properties

Address | Lease

IP Address: 172.21.0.5

Client Name: blue-labws

Owned by Server: blue-ncc1701

Configuration Macro: blue-ncc1701

Comment: Lab workstation

OK | Reset | Cancel | Help

Die folgende Abbildung zeigt das Dialogfeld „Mehrere Adressen ändern", in dem Sie mehrere IP-Adressen gleichzeitig ändern können.

ABBILDUNG 15–11 Dialogfeld „Mehrere Adressen ändern" in DHCP Manager

Modify Multiple Addresses

Number of Addresses Selected: 4

Managing Server: Keep current settings

Comment: Keep current settings

Configuration Macro: Keep current settings

BootP: Keep current settings

Assign all addresses only to BootP clients

Do not assign addresses to BootP clients

Unusable: Keep current settings

Mark all addresses unusable

Mark all addresses usable

Lease Type: Keep current settings

Dynamic

Permanent

OK | Reset | Cancel | Help

▼ So ändern Sie die Eigenschaften von IP-Adressen (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Adressen".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie das Netzwerk der IP-Adresse.**

3. **Wählen Sie eine oder mehrere zu ändernde IP-Adressen.**

   Wenn Sie mehrere Adressen ändern möchten, drücken Sie die Strg-Taste, während Sie mit der Maus auf die einzelnen Adressen klicken. Sie können auch die Umschalttaste gedrückt halten, um einen Adressblock zu markieren.

4. **Wählen Sie „Eigenschaften" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Eigenschaften für Adresse" oder „Mehrere Adressen ändern" wird angezeigt.

5. **Ändern Sie die gewünschten Eigenschaften.**

   Klicken Sie auf die Schaltfläche „Hilfe", oder suchen Sie in Tabelle 15–4 nach Informationen zu den Eigenschaften.

6. **Klicken Sie auf „OK".**

▼ So ändern Sie die Eigenschaften von IP-Adressen (`pntadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Ändern Sie die Eigenschaften einer IP-Adresse, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

   ```
   # pntadm -M ip-address options network-address
   ```

   Mit dem Befehl `pntadm` können verschiedene Optionen verwendet werden, die in der Manpage `pntadm(1M)` dokumentiert sind.

Tabelle 15–4 enthält einige Beispiele für `pntadm`, mit denen Optionen angegeben werden können.

Löschen von IP-Adressen aus dem DHCP-Service

Manchmal soll der DHCP-Service eine bestimmte IP-Adresse oder eine Gruppe von IP-Adressen nicht mehr verwalten. Die Methode, die Sie zum Löschen eine Adresse aus DHCP verwenden, hängt davon ab, ob diese Änderung nur vorübergehend oder permanent sein soll.

- Um die Verwendung bestimmter Adressen nur vorübergehend zu verhindern, kennzeichnen Sie die Adressen im Dialogfeld „Eigenschaften für Adresse" als „Nicht verwendbar". Dies wird unter „Kennzeichnen von IP-Adressen als nicht durch den DHCP-Service verwendbar" auf Seite 413 beschrieben.
- Um die Verwendung bestimmter Adressen durch DHCP-Clients permanent zu verhindern, löschen Sie die Adressen aus den DHCP-Netzwerktabellen. Dies wird unter „Löschen von IP-Adressen vom DHCP-Service" auf Seite 415 beschrieben.

Kennzeichnen von IP-Adressen als nicht durch den DHCP-Service verwendbar

Mit dem Befehl `pntadm -M` und der Option `-f UNUSABLE` können Sie bestimmte Adressen als nicht verwendbar kennzeichnen.

In DHCP Manager verwenden Sie das Dialogfeld „Eigenschaften für Adresse" (siehe Abbildung 15–10), um einzelne Adressen zu kennzeichnen. Mit dem Dialogfeld „Mehrere Adressen ändern" (siehe Abbildung 15–11) können Sie mehrere Adressen kennzeichnen. Dies wird im folgenden Verfahren beschrieben.

▼ So kennzeichnen Sie IP-Adressen als nicht verwendbar (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Adressen".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie das Netzwerk der IP-Adresse.**

3. **Wählen Sie eine oder mehrere IP-Adressen aus, die als nicht verwendbar gekennzeichnet werden sollen.**

   Wenn Sie mehrere Adressen als nicht verwendbar kennzeichnen möchten, drücken Sie die Strg-Taste, während Sie mit der Maus auf die einzelnen Adressen klicken. Sie können auch die Umschalttaste gedrückt halten, um einen Adressblock zu markieren.

4. **Wählen Sie „Eigenschaften" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Eigenschaften für Adresse" oder „Mehrere Adressen ändern" wird angezeigt.

5. **Wenn Sie eine Adresse ändern, wählen Sie die Registerkarte „Leasing".**

6. **Wählen Sie „Adresse ist nicht verwendbar".**

   Wenn Sie mehrere Adressen bearbeiten, wählen Sie „Alle Adressen als nicht verwendbar kennzeichnen".

7. **Klicken Sie auf „OK".**

▼ So kennzeichnen Sie IP-Adressen als nicht verwendbar (`pntadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Kennzeichnen Sie IP-Adressen als nicht verwendbar, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

   ```
   # pntadm -M ip-address -f UNUSABLE network-address
   ```

   Um beispielsweise die Adresse `10.64.3.3` als nicht verwendbar zu kennzeichnen, geben Sie den folgenden Befehl ein:

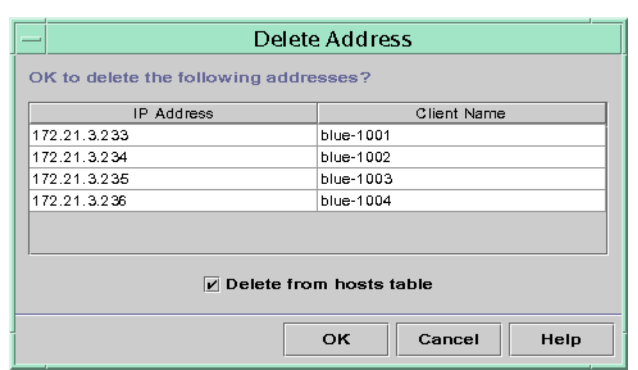
   ```
   pntadm -M 10.64.3.3 -f UNUSABLE 10.64.3.0
   ```

Löschen von IP-Adressen vom DHCP-Service

Sie können IP-Adressen aus den DHCP-Netzwerktabellen löschen, wenn diese Adressen nicht mehr von DHCP verwaltet werden sollen. Hierzu verwenden Sie den Befehl `pntadm -D` oder das Dialogfeld „Adresse löschen" in DHCP Manager.

Die folgende Abbildung zeigt das Dialogfeld „Adresse löschen".

ABBILDUNG 15–12 Dialogfeld „Adresse löschen" in DHCP Manager



▼ So löschen Sie IP-Adressen vom DHCP-Service (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Adressen".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie das Netzwerk der IP-Adresse.**

3. **Wählen Sie eine oder mehrere zu löschende IP-Adressen.**

   Wenn Sie mehrere Adressen löschen möchten, drücken Sie die Strg-Taste, während Sie mit der Maus auf die einzelnen Adressen klicken. Sie können auch die Umschalttaste gedrückt halten, um einen Adressblock zu markieren.

4. **Wählen Sie „Löschen" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Adresse löschen" enthält eine Liste der von Ihnen ausgewählten Adressen, so dass Sie den Löschvorgang bestätigen können.

5. **Wenn Sie die Hostnamen aus der hosts-Tabelle löschen möchten, wählen Sie „Aus Tabelle 'hosts' löschen".**

   Wenn die Hostnamen von DHCP Manager erzeugt wurden, müssen Sie die Namen eventuell aus der hosts-Tabelle löschen.

6. **Klicken Sie auf „OK".**

▼ So löschen Sie IP-Adressen vom DHCP-Service (`pntadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Löschen Sie IP-Adressen, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

   ```
   # pntadm -D ip-address options network-address
   ```

   Wenn Sie die Option `-y` hinzufügen, wird der Hostname aus dem Namen-Service gelöscht, der den Hostnamen verwaltet.

   Um beispielsweise die Adresse `10.64.3.3` aus dem Netzwerk `10.64.3.0` und den entsprechenden Hostnamen zu löschen, geben Sie den folgenden Befehl ein:

   ```
   pntadm -D 10.64.3.3 -y 10.64.3.0
   ```

Zuweisen einer reservierten IP-Adresse zu einem DHCP-Client

Der Oracle Solaris DHCP-Service versucht, einem Client die gleiche IP-Adresse bereitzustellen, die der Client zuvor über DHCP bezogen hat. Manchmal wurde eine Adresse jedoch bereits einem anderen Client zugewiesen.

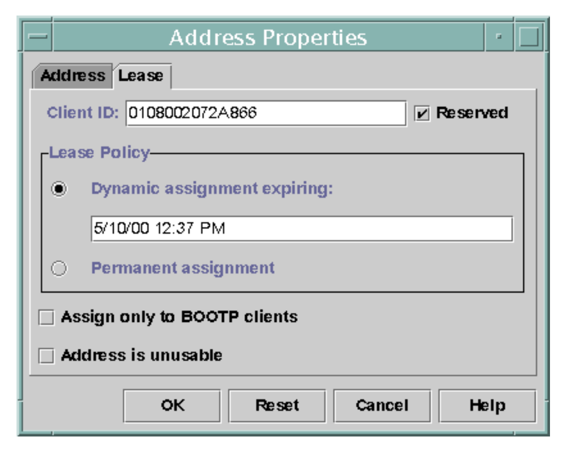
Router, NIS- oder NIS+-Server, DNS-Server und andere Hosts, die für ein Netzwerk wichtig sind, sollten keine DHCP-Clients werden. Hosts, die einem Netzwerk Services bereitstellen, dürfen sich nicht auf das Netzwerk verlassen, um ihre IP-Adressen zu beziehen. Clients wie z. B. Druck- oder Dateiserver müssen ebenfalls über konsistente IP-Adressen verfügen. Diese Clients beziehen ihre Netzwerkkonfigurationen vom DHCP-Server, der ihnen auch eine konsistente IP-Adresse zuweist.

Sie können den DHCP-Server so einrichten, dass er einem Client, der seine Konfiguration anfordert, jedes Mal die gleiche IP-Adresse zuweist. Sie reservieren die IP-Adresse für den Client, indem Sie die Client-ID manuell der Adresse zuweisen, die der Client verwenden soll. Sie können die reservierte Adresse entweder als dynamisches Leasing oder als permanentes Leasing einrichten. Wenn dynamisches Leasing für die Clientadresse verwendet wird, können Sie die Verwendung der Adresse leichter verfolgen. Ein festplattenloser Client sollte beispielsweise eine reservierte Adresse mit dynamischem Leasing verwenden. Bei permanentem Leasing für die Clientadresse können Sie die Verwendung der Adresse nicht verfolgen. Nachdem ein Client eine permanent geleaste Adresse bezogen hat, kontaktiert der Client den Server nicht noch einmal. Der Client kann nur dann aktualisierte Konfigurationsinformationen beziehen, wenn er die IP-Adresse freigibt und die Aushandlung für das DHCP-Leasing neu startet.

Die Leasing-Eigenschaften können Sie mit dem Befehl `pntadm -M` oder in dem Dialogfeld „Eigenschaften für Adresse" in DHCP Manager einrichten.

Die folgende Abbildung zeigt die Registerkarte „Leasing" im Dialogfeld „Eigenschaften für Adresse", die zum Ändern der Leasing-Eigenschaften verwendet wird.

ABBILDUNG 15–13 Registerkarte „Leasing" im Dialogfeld „Eigenschaften für Adresse" in DHCP Manager



▼ So weisen Sie einem DHCP-Client eine konsistente IP-Adresse zu (DHCP Manager)

1 Wählen Sie in DHCP Manager die Registerkarte „Adressen".

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie das entsprechende Netzwerk.**

3. **Doppelklicken Sie auf die IP-Adresse, die der Client verwenden soll.**

   Das Fenster „Eigenschaften für Adresse" wird angezeigt.

4. **Wählen Sie die Registerkarte „Leasing".**

5. **Geben Sie die Client-ID in das Feld „Client-ID" ein.**

   Die Client-ID wird von der Hardwareadresse des Clients abgeleitet. Weitere Informationen finden Sie unter dem Eintrag für die Client-ID in Tabelle 15–4.

6. **Wählen Sie die Option „Reserviert", um zu verhindern, dass die IP-Adresse vom Server zurückgefordert wird.**

7. **Wählen Sie im Bereich „Leasing-Policy" entweder eine dynamische oder eine permanente Zuweisung.**

   Wählen Sie eine dynamische Zuweisung, wenn der Client Leasings neu aushandeln soll. Dadurch können Sie die Verwendung der Adresse verfolgen. Da Sie „Reserviert" ausgewählt haben, kann die Adresse auch dann nicht zurückgefordert werden, wenn dynamisches Leasing verwendet wird. Sie müssen kein Ablaufdatum für dieses Leasing angeben. Der DHCP-Server berechnet das Ablaufdatum über die Leasing-Zeit.

   Wenn Sie ein permanentes Leasing wählen, können Sie die Verwendung der IP-Adresse nicht verfolgen, es sei denn, Sie aktivieren die Transaktionsprotokollierung.

8. **Klicken Sie auf „OK".**

▼ So weisen Sie einem DHCP-Client eine konsistente IP-Adresse zu (`pntadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Konfigurieren Sie die Leasing-Flags, indem Sie einen Befehl in der folgenden Syntax eingeben:**

   ```
   # pntadm -M ip-address -i client-id -f MANUAL+BOOTP network-address
   ```

Um beispielsweise den Solaris DHCP-Client mit der MAC-Adresse `08:00:20:94:12:1E` so einzurichten, dass er immer die IP-Adresse `10.21.5.12` erhält, geben Sie den folgenden Befehl ein:

```
pntadm -M 10.21.5.12 -i 0108002094121E -f MANUAL+BOOTP 10.21.0.0
```

Tipp – Weitere Informationen zum Ermitteln der Client-IDs finden Sie im Eintrag für die Client-ID in Tabelle 15–4.

Arbeiten mit DHCP-Makros (Übersicht der Schritte)

DHCP-Makros sind Container für DHCP-Optionen. Der Oracle Solaris DHCP-Service verwendet Makros, um Optionen zusammenzufassen, die an Clients übergeben werden sollen. DHCP Manager und das Dienstprogramm `dhcpconfig` erstellen bei der Konfiguration des Servers automatisch verschiedene Makros. Hintergrundinformationen zu Makros finden Sie unter „Einführung in DHCP-Makros" auf Seite 334 Informationen zu den standardmäßig erstellten Makros finden Sie unter Kapitel 14, „Konfiguration des DHCP-Services (Aufgaben)".

Bei Änderungen in Ihrem Netzwerk kann es erforderlich werden, dass die Konfigurationsinformationen, die an die Clients übergeben wurden, geändert werden müssen. Dazu verwenden Sie die DHCP-Makros. DHCP-Makros können Sie anzeigen, erstellen, ändern, duplizieren und löschen.

Zum Arbeiten mit Makros, müssen Sie mit den DHCP-Standardoptionen vertraut sein, die in der Manpage `dhcp_inittab(4)` beschrieben sind.

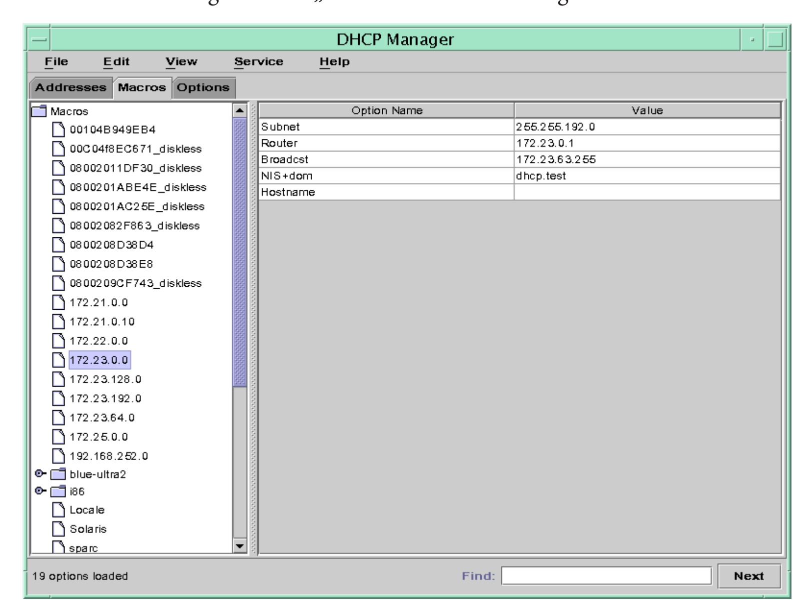
In der folgenden Tabelle sind die Aufgaben aufgeführt, mit denen Sie DHCP-Makros anzeigen, erstellen, ändern und löschen können. Außerdem enthält die Tabelle Links zu den Abschnitten, in denen die Ausführung der einzelnen Aufgaben beschrieben ist.

Aufgabe	Beschreibung	Siehe
Anzeigen von DHCP-Makros.	Zeigen Sie eine Liste aller Makros an, die auf dem DHCP-Server definiert sind.	„So zeigen Sie die auf einem DHCP-Server definierten Makros an (DHCP Manager)" auf Seite 421 „So zeigen Sie die auf einem DHCP-Server definierten Makros an (`dhtadm`)" auf Seite 421
Erstellen von DHCP-Makros.	Erstellen Sie neue Makros, um DHCP-Clients zu unterstützen.	„So erstellen Sie ein DHCP-Makro (DHCP Manager)" auf Seite 427 „So erstellen Sie ein DHCP-Makro (`dhtadm`)" auf Seite 428

Aufgabe	Beschreibung	Siehe
Ändern der Werte, die in Makros an DHCP-Clients übergeben werden.	Ändern Sie Makros, indem Sie vorhandene Optionen bearbeiten, neue Optionen zu Makros hinzufügen oder Optionen aus Makros entfernen.	„So ändern Sie die Werte für Optionen in einem DHCP-Makro (DHCP Manager)" auf Seite 422 „So ändern Sie die Werte für Optionen in einem DHCP-Makro (`dhtadm`)" auf Seite 423 „So fügen Sie Optionen zu einem DHCP-Makro hinzu (DHCP Manager)" auf Seite 424 „So fügen Sie Optionen zu einem DHCP-Makro hinzu (`dhtadm`)" auf Seite 425 „So löschen Sie Optionen aus einem DHCP-Makro (DHCP Manager)" auf Seite 425 „So löschen Sie Optionen aus einem DHCP-Makro (`dhtadm`)" auf Seite 426
Löschen von DHCP-Makros.	Löschen Sie nicht mehr benötigte DHCP-Makros.	„So löschen Sie ein DHCP-Makro (DHCP Manager)" auf Seite 429 „So löschen Sie ein DHCP-Makro (`dhtadm`)" auf Seite 429

In der folgenden Abbildung wird die Registerkarte „Makros" in DHCP Manager gezeigt.

ABBILDUNG 15–14 Registerkarte „Makros" in DHCP Manager



So zeigen Sie die auf einem DHCP-Server definierten Makros an (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Makros".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

   Im Bereich „Makros" links im Fenster werden alle auf dem DHCP-Server definierten Makros in alphabetischer Reihenfolge angezeigt. Makros, die durch ein Ordnersymbol gekennzeichnet sind, beinhalten Verweise auf andere Makros, während durch ein Dokumentsymbol gekennzeichnete Makros nicht auf andere Makros verweisen.

2. **Um einen Makroordner zu öffnen, klicken Sie auf das Symbol links neben dem Ordnersymbol.**

   Die in dem ausgewählten Makro enthaltenen Makros werden aufgeführt.

3. **Klicken Sie auf einen Makronamen, um den Inhalt des Makros anzuzeigen.**

   Optionen und deren zugewiesenen Werte werden angezeigt.

So zeigen Sie die auf einem DHCP-Server definierten Makros an (`dhtadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Zeigen Sie die Makros an, indem Sie den folgenden Befehl eingeben:**

   ```
   # dhtadm -P
   ```

   Mit diesem Befehl wird der formatierte Inhalt der `dhcptab`-Tabelle einschließlich aller auf dem DHCP-Server definierten Makros und Symbole über das standardmäßige Ausgabegerät gedruckt.

Ändern von DHCP-Makros

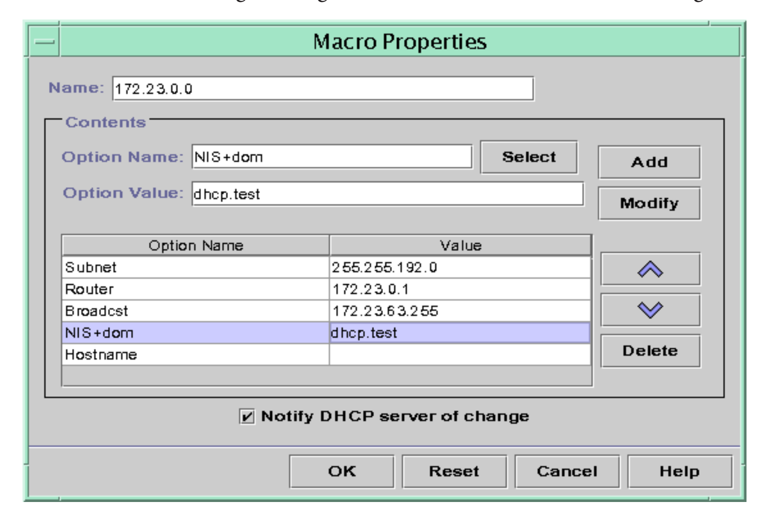
Eventuell müssen Sie Änderungen an Makros vornehmen, wenn sich bestimmte Aspekte Ihres Netzwerks ändern und DHCP-Clients über diese Änderung informiert werden müssen. Angenommen, Sie fügen einen Router oder einen NIS-Server hinzu, erstellen ein neues Teilnetz oder ändern die Leasing-Richtlinie.

Bevor Sie ein Makro ändern, ermitteln Sie den Namen der DHCP-Option, die Sie ändern, hinzufügen oder löschen möchten. Die standardmäßige DHCP-Optionen sind in der DHCP Manager-Hilfe und in der Manpage `dhcp_inittab(4)` aufgeführt.

Zum Ändern von Makros können Sie den Befehl `dhtadm -M -m` oder DHCP Manager verwenden. Weitere Informationen zum Befehl `dhtadm(1M)` finden Sie in der Manpage `dhtadm` .

Die folgende Abbildung zeigt das Dialogfeld „Eigenschaften für Makro" in DHCP Manager.

ABBILDUNG 15–15 Dialogfeld „Eigenschaften für Makro" in DHCP Manager



So ändern Sie die Werte für Optionen in einem DHCP-Makro (DHCP Manager)

1 Wählen Sie in DHCP Manager die Registerkarte „Makros".

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2 Wählen Sie das Makro, das Sie ändern möchten.

3 **Wählen Sie „Eigenschaften" im Menü „Bearbeiten" aus.**

Das Dialogfeld „Eigenschaften für Makro" wird angezeigt.

4 **Wählen Sie die zu ändernde Option in der Optionstabelle aus.**

Der Name der Option und der zugehörige Wert werden in den Feldern „Optionsname" und „Optionswert" angezeigt.

5 **Markieren Sie im Feld „Optionswert" den alten Wert und geben Sie den neuen Wert für die Option ein.**

6 **Klicken Sie auf „Ändern".**

Der neue Wert wird in der Optionstabelle angezeigt.

7 **Aktivieren Sie das Kontrollkästchen „DHCP-Server von Änderung benachrichtigen".**

Diese Auswahl weist den DHCP-Server an, die `dhcptab`-Tabelle erneut einzulesen, um die darin vorgenommenen Änderungen unmittelbar nach dem Klicken auf „OK" zu übernehmen.

8 **Klicken Sie auf „OK".**

▼ So ändern Sie die Werte für Optionen in einem DHCP-Makro (`dhtadm`)

1 **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 **Ändern Sie die Optionswerte, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

```
# dhtadm -M -m macroname -e 'option=value:option=value' -g
```

Um beispielsweise die Leasing-Zeit und den Universal Time Offset im Makro `bluenote` zu ändern, geben Sie den folgenden Befehl ein:

```
# dhtadm -M -m bluenote -e 'LeaseTim=43200:UTCOffst=28800' -g
```

▼ So fügen Sie Optionen zu einem DHCP-Makro hinzu (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Makros".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie das Makro, das Sie ändern möchten.**

3. **Wählen Sie „Eigenschaften" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Eigenschaften für Makro" wird angezeigt.

4. **Geben Sie mithilfe einer der folgenden Methoden den Namen der Option in das Feld „Optionsname" ein**

   - **Klicken Sie neben dem Feld „Optionsname" auf die Schaltfläche „Auswählen", um eine Option auszuwählen, die dem Makro hinzugefügt werden soll.**

     Das Dialogfeld „Option wählen" enthält eine alphabetisch sortierte Liste mit den Namen der Optionen der Standardkategorie sowie Beschreibungen. Wenn Sie eine Option hinzufügen möchten, die nicht in der Standardkategorie enthalten ist, wählen Sie eine Kategorie in der Liste „Kategorie" aus.

     Weitere Informationen zu Makrokategorien finden Sie unter „Einführung in DHCP-Makros" auf Seite 334.

   - **Geben Sie `Include` ein, wenn Sie einen Verweis auf ein vorhandenes Makro in das neue Makro aufnehmen möchten.**

5. **Geben Sie den Wert für die Option in das Feld „Optionswert" ein.**

   Wenn Sie **`Include`** als Optionsnamen eingegeben haben, müssen Sie den Namen eines vorhandenen Makros in das Feld „Optionswert" eintragen.

6. **Klicken Sie auf „Hinzufügen".**

   Die Option wird am Ende der Optionsliste in dieses Makro eingefügt. Um die Position der Option im Makro zu ändern, markieren Sie die Option und klicken auf die Pfeilschaltfläche, um die Option nach oben oder unten zu verschieben.

7. **Aktivieren Sie das Kontrollkästchen „DHCP-Server von Änderung benachrichtigen".**

   Diese Auswahl weist den DHCP-Server an, die `dhcptab`-Tabelle erneut einzulesen, um die darin vorgenommenen Änderungen unmittelbar nach dem Klicken auf „OK" zu übernehmen.

8. **Klicken Sie auf „OK".**

▼ So fügen Sie Optionen zu einem DHCP-Makro hinzu (`dhtadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Fügen Sie einem Makro Optionen hinzu, indem Sie einen Befehl im folgenden Format eingeben:**

   ```
   # dhtadm -M -m macroname -e 'option=value' -g
   ```

   Um beispielsweise die Fähigkeit zur Aushandlung von Leasings zum Makro `bluenote` hinzuzufügen, geben Sie den folgenden Befehl ein:

   ```
   # dhtadm -M -m bluenote -e 'LeaseNeg=_NULL_VALUE' -g
   ```

   Wenn eine Option keinen Wert benötigt, müssen Sie `_NULL_VALUE` als Wert für die Option verwenden.

▼ So löschen Sie Optionen aus einem DHCP-Makro (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Makros“.**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

2. **Wählen Sie das Makro, das Sie ändern möchten.**

3. **Wählen Sie „Eigenschaften“ im Menü „Bearbeiten“ aus.**

   Das Dialogfeld „Eigenschaften für Makro“ wird angezeigt.

4. **Wählen Sie die Option aus, die Sie löschen möchten.**

5. **Klicken Sie auf „Löschen“.**

   Die Option wird aus der Optionsliste für dieses Makro entfernt.

6. **Aktivieren Sie das Kontrollkästchen „DHCP-Server von Änderung benachrichtigen".**

   Diese Auswahl weist den DHCP-Server an, die `dhcptab`-Tabelle erneut einzulesen, um die darin vorgenommenen Änderungen unmittelbar nach dem Klicken auf „OK" zu übernehmen.

7. **Klicken Sie auf „OK".**

▼ So löschen Sie Optionen aus einem DHCP-Makro (`dhtadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Löschen Sie eine Option aus einem Makro, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

   ```
   # dhtadm -M -m macroname -e 'option=' -g
   ```

   Um beispielsweise die Fähigkeit zur Aushandlung von Leasings aus dem Makro `bluenote` zu löschen, geben Sie den folgenden Befehl ein:

   ```
   # dhtadm -M -m bluenote -e 'LeaseNeg=' -g
   ```

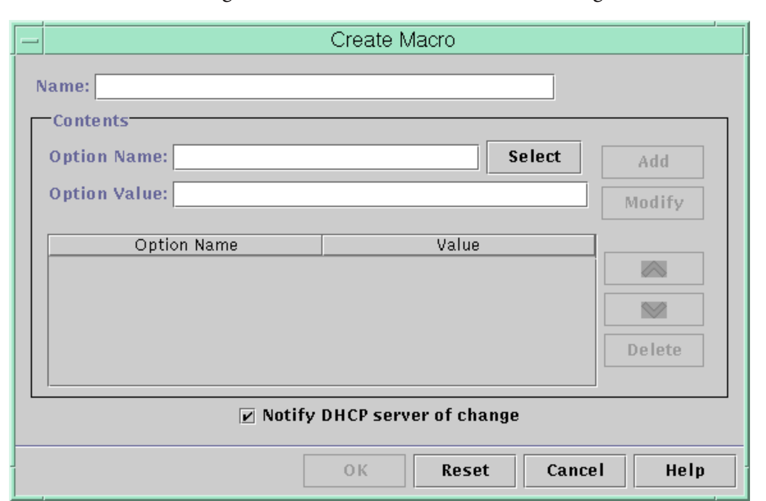
   Wenn eine Option ohne einen Wert angegeben wird, wird die Option aus dem Makro entfernt.

Erstellen von DHCP-Makros

Eventuell möchten Sie neue Makros zu Ihrem DHCP-Service hinzufügen, um Clients mit bestimmten Anforderungen zu unterstützen. Zum Erstellen von Makros können Sie den Befehl `dhtadm -A -m` oder das Dialogfeld „Makro erstellen" in DHCP Manager verwenden. Weitere Informationen zum Befehl `dhtadm` finden Sie in der Manpage `dhtadm(1M)`.

Die folgende Abbildung zeigt das Dialogfeld „Makro erstellen" in DHCP Manager.

ABBILDUNG 15–16 Dialogfeld „Makro erstellen" in DHCP Manager



So erstellen Sie ein DHCP-Makro (DHCP Manager)

1 Wählen Sie in DHCP Manager die Registerkarte „Makros".

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2 Wählen Sie „Erstellen" im Menü „Bearbeiten" aus.

Das Dialogfeld „Makro erstellen" wird angezeigt.

3 Geben Sie einen einmaligen Namen für das Makro ein.

Der Name kann bis zu 128 alphanumerischen Zeichen umfassen. Wenn Sie einen Namen verwenden, der einem Hersteller-Klassenbezeichner, einer Netzwerkadresse oder einer Client-ID entspricht, wird das Makro automatisch für die entsprechenden Clients verarbeitet. Wenn Sie einen anderen Namen eingeben, wird das Makro nicht automatisch verarbeitet. Das Makro muss einer bestimmten IP-Adresse zugewiesen oder in ein anderes Makro eingefügt werden, das automatisch verarbeitet wird. Ausführliche Informationen finden Sie unter „Von DHCP-Server verarbeitete Makros" auf Seite 334.

4 Klicken Sie neben dem Feld „Optionsname" auf die Schaltfläche „Auswählen".

Das Dialogfeld „Option wählen" enthält eine alphabetisch sortierte Liste mit den Namen der Optionen der Standardkategorie sowie Beschreibungen. Wenn Sie eine Option hinzufügen möchten, die nicht in der Standardkategorie enthalten ist, verwenden Sie die Liste „Kategorie". Wählen Sie die gewünschte Kategorie in der Liste „Kategorie" aus. Weitere Informationen zu Optionskategorien finden Sie unter „Einführung in DHCP-Optionen" auf Seite 333.

5. **Wählen Sie die Option aus, die dem Makro hinzugefügt werden soll, und klicken Sie auf „OK".**

   Das Dialogfeld „Eigenschaften für Makro" zeigt die ausgewählte Option im Feld „Optionsname" an.

6. **Geben Sie den Wert für die Option in das Feld „Optionswert" ein, und klicken Sie auf „Hinzufügen".**

   Die Option wird am Ende der Optionsliste in dieses Makro eingefügt. Um die Position der Option im Makro zu ändern, markieren Sie die Option und klicken auf die Pfeilschaltfläche, um die Option nach oben oder unten zu verschieben.

7. **Wiederholen Sie Schritt 5 und Schritt 6 für jede Option, die Sie dem Makro hinzufügen möchten.**

8. **Aktivieren Sie das Kontrollkästchen „DHCP-Server von Änderung benachrichtigen", wenn Sie keine weiteren Optionen mehr hinzufügen möchten.**

   Diese Auswahl weist den DHCP-Server an, die `dhcptab`-Tabelle erneut einzulesen, um die darin vorgenommenen Änderungen unmittelbar nach dem Klicken auf „OK" zu übernehmen.

9. **Klicken Sie auf „OK".**

▼ So erstellen Sie ein DHCP-Makro (`dhtadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Erstellen Sie ein Makro, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

   ```
   # dhtadm -A -m macroname -d ':option=value:option=value:option=value:' -g
   ```

   Es gibt keinen Grenzwert für die Anzahl an *Option*=*Wert*-Paaren, die in dem Argument für `-d` enthalten sein können. Das Argument muss mit einem Doppelpunkt beginnen und enden, und es muss sich zwischen jedem *Option*=*Wert*-Paar ein Doppelpunkt befinden. Der vollständige String muss in Anführungszeichen eingeschlossen sein.

   Um beispielsweise das Makro `bluenote` zu erstellen, geben Sie den folgenden Befehl ein:

   ```
   # dhtadm -A -m bluenote -d ':Router=10.63.6.121\
   :LeaseNeg=_NULL_VALUE:DNSserv=10.63.28.12:' -g
   ```

Wenn eine Option keinen Wert benötigt, müssen Sie `_NULL_VALUE` als Wert für die Option verwenden.

Löschen von DHCP-Makros

Eventuell müssen Sie ein Makro aus dem DHCP-Service löschen. Wenn Sie beispielsweise ein Netzwerk aus dem DHCP-Service löschen, können Sie auch das dazugehörige Netzwerkmakro löschen.

Zum Löschen von Makros können Sie den Befehl `dhtadm -D -m` oder DHCP Manager verwenden.

▼ So löschen Sie ein DHCP-Makro (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Makros".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie das zu löschende Makro aus.**

   Das Dialogfeld „Makro löschen" fordert Sie zur Bestätigung auf, dass Sie das angegebene Makro löschen möchten.

3. **Aktivieren Sie das Kontrollkästchen „DHCP-Server von Änderung benachrichtigen".**

   Diese Auswahl weist den DHCP-Server an, die `dhcptab`-Tabelle erneut einzulesen, um die darin vorgenommenen Änderungen unmittelbar nach dem Klicken auf „OK" zu übernehmen.

4. **Klicken Sie auf „OK".**

▼ So löschen Sie ein DHCP-Makro (`dhtadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Löschen Sie ein Makro, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

```
# dhtadm -D -m macroname -g
```

Um beispielsweise das Makro `bluenote` zu löschen, geben Sie den folgenden Befehl ein:

```
# dhtadm -D -m bluenote -g
```

Arbeiten mit DHCP-Optionen (Übersicht der Schritte)

Optionen sind Schlüsselwörter für Netzwerkkonfigurationsparameter, die der DHCP-Server an Clients übergeben kann. Im Oracle Solaris DHCP-Service können Sie die standardmäßige DHCP-Optionen weder erstellen, löschen noch ändern. Die Standardoptionen werden von DHCP-Protokoll definiert, daher können die Optionen nicht geändert werden. Aufgaben können Sie nur an Optionen durchführen, die Sie für Ihren Standort erstellt haben. Aus diesem Grund ist die Registerkarte „Optionen" in DHCP Manager bei der Erstkonfiguration des DHCP-Services leer, bis Sie Optionen für Ihren Standort erstellt haben.

Wenn Sie Optionen auf dem DHCP-Server erstellen, müssen Sie auch Informationen zu den Optionen auf dem DHCP-Client hinzufügen. Beim Oracle Solaris DHCP-Client müssen Sie der Datei `/etc/dhcp/inittab` Einträge für die neuen Optionen hinzufügen. Weitere Informationen zu dieser Datei finden Sie in der Manpage `dhcp_inittab(4)`.

Bei DHCP-Clients, bei denen es sich nicht um Oracle Solaris-Clients handelt, suchen Sie in der Dokumentation nach Informationen zum Hinzufügen von Optionen bzw. Symbolen. Weitere Informationen zu Optionen in Oracle Solaris DHCP finden Sie unter „Einführung in DHCP-Optionen" auf Seite 333.

Zum Erstellen, Ändern oder Löschen von Optionen können Sie entweder DHCP Manager oder den Befehl `dhtadm` verwenden.

Tipp – In der DHCP-Literatur werden Optionen auch als *Symbole* bezeichnet. Auch der Befehl `dhtadm` und die dazugehörige Manpage verwendet den Begriff Symbole für Optionen.

In der folgenden Tabelle sind die Aufgaben aufgeführt, die Sie zum Erstellen, Ändern und Löschen von DHCP-Optionen ausführen müssen. Die Tabelle enthält Links zu den Verfahren, in denen die Ausführung der Aufgaben beschrieben wird.

Aufgabe	Beschreibung	Siehe
Erstellen von DHCP-Optionen.	Fügen Sie neue Optionen für Informationen hinzu, die nicht durch eine standardmäßige DHCP-Option abgedeckt sind.	„So erstellen Sie DHCP-Optionen (DHCP Manager)" auf Seite 434 „So erstellen Sie DHCP-Optionen (`dhtadm`)" auf Seite 435 „Ändern der Optionsinformationen eines Oracle Solaris DHCP-Client" auf Seite 439

Aufgabe	Beschreibung	Siehe
Ändern von DHCP-Optionen.	Ändern Sie die Eigenschaften der von Ihnen erstellten DHCP-Optionen.	„So ändern Sie die Eigenschaften einer DHCP-Option (DHCP Manager)“ auf Seite 436 „So ändern Sie die Eigenschaften einer DHCP-Option (`dhtadm`)“ auf Seite 437
Löschen von DHCP Optionen.	Löschen Sie die von Ihnen erstellten DHCP-Optionen.	„So löschen Sie DHCP-Optionen (DHCP Manager)“ auf Seite 438 „So löschen Sie DHCP-Optionen (`dhtadm`)“ auf Seite 439

Bevor Sie DHCP-Optionen erstellen, müssen Sie sich mit den Eigenschaften der Optionen vertraut machen, die in der folgenden Tabelle aufgeführt sind.

TABELLE 15–5 Eigenschaften von DHCP-Optionen

Optionseigenschaft	Beschreibung
Kategorie	Die *Kategorie* einer Option muss eine der folgenden sein: ■ Anbieter – Optionen, die nur für die Herstellerplattform eines Clients gelten, entweder Hardware oder Software. ■ Standort – Optionen, die nur für Ihren Standort gelten. ■ Erweitert – Neuere Optionen, die dem DHCP-Protokoll hinzugefügt wurden, aber noch nicht als Standardoptionen in Oracle Solaris DHCP umgesetzt sind.
Code	Der *Code* ist eine einmalige Zahl, die Sie einer Option zuweisen. Sie können den gleichen Code keiner anderen Option innerhalb dieser Optionskategorie zuweisen. Der Code muss für die Optionskategorie geeignet sein: ■ Anbieter – Codewerte zwischen 1–254 für jede Hersteller-Klasse ■ Standort – Codewerte zwischen 128–254 ■ Erweitert – Codewerte zwischen 77–127

TABELLE 15–5 Eigenschaften von DHCP-Optionen *(Fortsetzung)*

Optionseigenschaft	Beschreibung
Datentyp	Der *Datentyp* gibt an, welche Daten einer Option als Wert zugeordnet werden können. Die gültigen Datentypen werden in der folgenden Liste beschrieben. ■ ASCII – Eine Textzeichenfolge. ■ Boolescher Wert – Dem Datentyp „Boolescher Wert" ist kein Wert zugeordnet. Das Vorhandensein dieser Option gibt an, dass eine Bedingung wahr ist, wenn diese Option nicht vorhanden ist, ist eine Begegnung falsch. Beispielsweise hat die Option `Hostname` den Datentyp „Boolescher Wert". Das Vorhandensein von `Hostname` in einem Makro führt dazu, dass der DHCP-Server den Hostnamen nachschlägt, der einer zugewiesenen Adresse zugeordnet ist. ■ IP – Eine oder mehrere IP-Adressen, in der getrennten dezimalen Notation (*xxx.xxx.xxx.xxx*). ■ Oketett – Nicht interpretierte ASCII-Darstellung von binären Daten. Beispielsweise wird der Datentyp „Oktett" von einer Client-ID verwendet. Zulässige Zeichen sind 0–9, A–F und a–f. Zur Darstellung einer 8-Bit-Quantität sind zwei ASCII-Zeichen erforderlich. ■ UNUMBER8, UNUMBER16, UNUMBER32, UNUMBER64, SNUMBER8, SNUMBER16, SNUMBER32 oder SNUMBER64 – Numerischer Wert. Ein einleitendes U oder S gibt an, ob die Zahl vorzeichenlos (unsigned) oder vorzeichenbehaftet (signed) ist. Die Zahlen am Ende geben an, wie viele Bit in der Zahl vorhanden sind.
Granularität	Die *Granularität* gibt an, wie viele „Instanzen" des Datentyps erforderlich sind, um einen vollständigen Optionswert darzustellen. Beispielsweise geben ein Datentyp „IP" und eine Granularität von 2 an, dass der Optionswert zwei IP-Adressen enthalten muss.
Maximum	Die Höchstzahl an Werten, die für eine Option angegeben werden können. Angenommen, Maximum ist 2, die Granularität ist 2 und der Datentyp ist IP. In diesem Fall kann der Optionswert maximal zwei Paare mit IP-Adressen enthalten.

TABELLE 15–5 Eigenschaften von DHCP-Optionen *(Fortsetzung)*

Optionseigenschaft	Beschreibung
Hersteller-Client-Klassen	Diese Option ist nur dann verfügbar, wenn die Optionskategorie „Anbieter" lautet. Die Hersteller-Client-Klassen kennzeichnen die Client-Klassen, denen die Option „Anbieter" zugeordnet ist. Die Klasse ist ein ASCII-String, der den Client-Computertyp oder das Betriebssystem darstellt. Beispielsweise ist der Klassen-String für einige Modelle der Sun-Workstations `SUNW.Sun-Blade-100` . Mit diesem Optionstyp können Sie Konfigurationsparameter definieren, die an alle Clients der gleichen Klasse und *nur* an Clients dieser Klasse übergeben werden. Sie können mehrere Client-Klassen angeben. Nur die DHCP-Clients, deren Client-Klassenwert der von Ihnen angegebenen Klasse entspricht, empfangen die Optionen für diese Klasse. Die Client-Klasse wird vom Hersteller des DHCP-Client festgelegt. Bei DHCP-Clients, bei denen es sich nicht um Oracle Solaris-Clients handelt, lesen Sie die Dokumentation des Herstellers für den DHCP-Client der jeweiligen Client-Klasse. Bei Solaris-Client kann die Vendor-Client-Klasse durch Eingabe des Befehls `uname -i` auf dem Client angezeigt werden. Zur Angabe der Hersteller-Client-Klasse ersetzen Sie die Kommas in dem vom Befehl `uname` zurückgegebenen String durch Punkte. Angenommen, der String `SUNW,Sun-Blade-100` wird von dem Befehl `uname -i` zurückgegeben, so geben Sie die Hersteller-Client-Klasse als `SUNW.Sun-Blade-100` an.

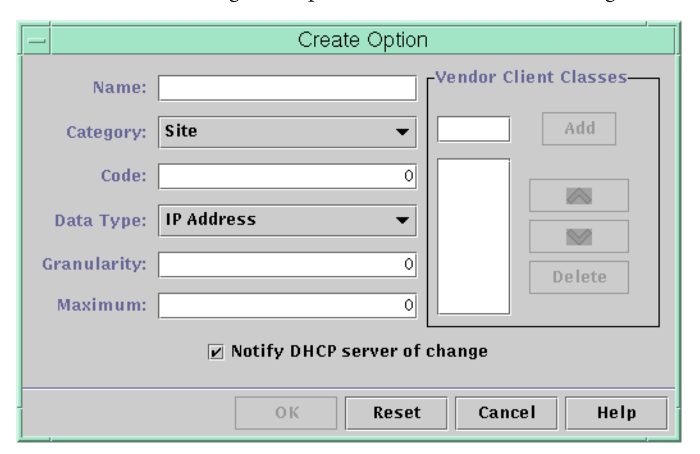
Erstellen von DHCP-Optionen

Wenn Sie Client-Informationen übergeben müssen, für die noch keine Option in DHCP-Protokoll existiert, können Sie eine Option erstellen. Bevor Sie Ihre eigene Option erstellen, prüfen Sie die Liste aller für Oracle Solaris DHCP erstellten Optionen in der Manpage `dhcp_inittab`(4).

Zum Erstellen von neuen Optionen können Sie den Befehl `dhtadm -A -s` oder das Dialogfeld „Option erstellen" in DHCP Manager verwenden.

Die folgende Abbildung zeigt das Dialogfeld „Option erstellen" in DHCP Manager.

ABBILDUNG 15–17 Dialogfeld „Option erstellen" in DHCP Manager



So erstellen Sie DHCP-Optionen (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Optionen".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie „Erstellen" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Optionen erstellen" wird angezeigt.

3. **Geben Sie einen kurzen beschreibenden Namen für die neue Option ein.**

   Der Name kann bis zu 128 alphanumerische Zeichen und Leerstellen umfassen.

4. **Wählen oder geben Sie Werte für jede Einstellung in das Dialogfeld ein.**

   Weitere Informationen zu den Einstellungen finden Sie in Tabelle 15–5 oder in der DHCP Manager-Hilfe.

5. **Aktivieren Sie das Kontrollkästchen „DHCP-Server von Änderung benachrichtigen", wenn Sie keine weiteren Optionen mehr erstellen möchten.**

   Diese Auswahl weist den DHCP-Server an, die `dhcptab`-Tabelle erneut einzulesen, um die darin vorgenommenen Änderungen unmittelbar nach dem Klicken auf „OK" zu übernehmen.

6. **Klicken Sie auf „OK".**

   Jetzt können Sie die Optionsmakros hinzufügen und der Option einen Wert zuweisen, der an Clients übergeben wird.

▼ So erstellen Sie DHCP-Optionen (`dhtadm`)

1 Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.

Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Erstellen Sie eine DHCP-Option, indem Sie einen Befehl mit der folgenden Syntax eingeben:

`# dhtadm -A -s` *option-name* `-d '`*category,code,data-type,granularity,maximum*`' -g`

Optionsname	Ist der alphanumerische String mit 128 oder weniger Zeichen.
Kategorie	Ist eine der Folgenden: `Site`, `Extend`, or `Vendor=`*Liste der Klassen*. *Liste-der-Klassen* ist eine durch Leerzeichen getrennte Liste der Hersteller-Client-Klassen, für die diese Option gilt. Informationen zum Feststellen der Hersteller-Client-Klasse finden Sie unter Tabelle 15–5.
Code	Ist ein nummerischer Wert, der für die Optionskategorie geeignet ist. Siehe dazu Tabelle 15–5
Datentyp	Gibt ein Schlüsselwort an, das den Datentyp kennzeichnet, der mit der Option übergeben wird. Siehe dazu Tabelle 15–5.
Granularität	Wird als eine nicht-negative Zahl angegeben. Siehe dazu Tabelle 15–5.
Maximum	Ist eine nicht-negative Zahl. Siehe dazu Tabelle 15–5.

Beispiel 15–3 Erstellen einer DHCP-Option mit `dhtadm`

Mit dem folgenden Befehl erstellen Sie eine Option namens `NewOpt`, bei der es sich um eine Option der Kategorie „Standort" handelt. Der Optionscode ist 130. Der Optionswert kann auf eine einzelne vorzeichenlose 8-Bit-Ganzzahl gesetzt werden.

```
# dhtadm -A -s NewOpt -d 'Site,130,UNUMBER8,1,1' -g
```

Der folgende Befehl erstellt eine Option namens `NewServ`, die zur Optionskategorie „Anbieter" gehört und für Clients gilt, deren Computertyp `SUNW,Sun-Blade-100` oder `SUNW,Sun-Blade-1000` ist. Der Optionscode ist 200. Der Optionswert kann auf eine IP-Adresse gesetzt werden.

```
# dhtadm -A -s NewServ -d 'Vendor=SUNW.Sun-Blade-100 \
SUNW.Sun-Blade-1000,200,IP,1,1' -g
```

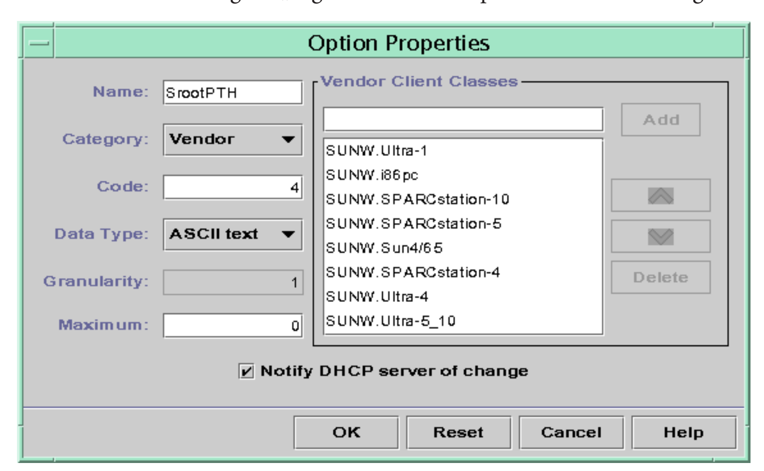
Ändern von DHCP-Optionen

Wenn Sie Optionen für Ihren DHCP-Service erstellt haben, können Sie die Eigenschaften dieser Optionen ändern. Zum Ändern von Optionen können Sie den Befehl `dhtadm -M -s` oder das Dialogfeld „Eigenschaften für Option" in DHCP Manager verwenden.

Sie müssen die Informationen der Oracle Solaris DHCP-Clientoption ändern, um die Änderungen widerzuspiegeln, die Sie am DHCP-Service vorgenommen haben. Lesen Sie dazu „Ändern der Optionsinformationen eines Oracle Solaris DHCP-Client" auf Seite 439.

Die folgende Abbildung zeigt das Dialogfeld „Eigenschaften für Option" in DHCP Manager.

ABBILDUNG 15–18 Dialogfeld „Eigenschaften für Option" in DHCP Manager



▼ So ändern Sie die Eigenschaften einer DHCP-Option (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Optionen".**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie die Option aus, die Sie ändern möchten.**

3. **Wählen Sie „Eigenschaften" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Eigenschaften für Option" wird angezeigt.

4 Nehmen Sie die erforderlichen Änderungen an den Eigenschaften vor.

Informationen zu den Eigenschaften finden Sie in Tabelle 15–5 oder in der DHCP Manager-Hilfe.

5 Aktivieren Sie das Kontrollkästchen „DHCP-Server von Änderung benachrichtigen", wenn Sie keine weiteren Optionen mehr ändern möchten.

Die Änderungen werden in die `dhcptab`-Tabelle übernommen. Der DHCP-Server wird angewiesen, die `dhcptab`-Tabelle neu einzulesen, um die Änderungen zu übernehmen.

6 Klicken Sie auf „OK".

▼ So ändern Sie die Eigenschaften einer DHCP-Option (`dhtadm`)

1 Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.

Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Ändern Sie eine Option, indem Sie einen Befehl mit der folgenden Syntax eingeben:

```
# dhtadm -M -s option-name -d 'category,code,data-type,granularity,maximum' -g
```

Optionsname	Gibt den Namen der zu ändernden Option an.
Kategorie	Kann entweder `Site`, `Extend` oder `Vendor=`*Liste-der-Klassen* sein. *Liste-der-Klassen* ist eine durch Leerzeichen getrennte Liste der Hersteller-Client-Klassen, für die diese Option gilt. Beispiel:`SUNW.Sun-Blade-100 SUNW.Ultra-80 SUNWi86pc`.
Code	Gibt einen nummerischen Wert an, der für die Optionskategorie geeignet ist. Siehe dazu Tabelle 15–5.
Datentyp	Gibt ein Schlüsselwort an, das den mit der Option übergebenen Datentyp kennzeichnet. Siehe dazu Tabelle 15–5.
Granularität	Ist eine nicht-negative Zahl. Siehe dazu Tabelle 15–5.
Maximum	Ist eine nicht-negative Zahl. Siehe dazu Tabelle 15–5.

Bei dem Flag `-d` müssen Sie alle Eigenschaften einer DHCP-Option angeben, nicht nur die Eigenschaften, die Sie ändern möchten.

Beispiel 15–4 Ändern einer DHCP-Option mit `dhtadm`

Mit dem folgenden Befehl ändern Sie eine Option namens `NewOpt` . Diese Option ist eine Option der Kategorie „Standort“. Der Optionscode ist 135. Der Optionswert kann auf eine einzelne vorzeichenlose 8-Bit-Ganzzahl gesetzt werden.

```
# dhtadm -M -s NewOpt -d 'Site,135,UNUMBER8,1,1'
```

Mit dem folgenden Befehl ändern Sie eine Option namens `NewServ`, bei der es sich um eine Option der Kategorie „Anbieter“ handelt. Diese Option gilt jetzt für Clients, deren Computertyp `SUNW,Sun-Blade-100` oder `SUNW,i86pc` ist. Der Optionscode ist 200. Der Optionswert kann auf eine IP-Adresse gesetzt werden.

```
# dhtadm -M -s NewServ -d 'Vendor=SUNW.Sun-Blade-100 \ SUNW.i86pc,200,IP,1,1' -g
```

Löschen von DHCP-Optionen

Standardmäßige DHCP-Optionen können nicht gelöscht werden. Wenn Sie jedoch Optionen für Ihren DHCP-Service definiert haben, können Sie diese Optionen entweder in DHCP Manager oder mit dem Befehl `dhtadm` löschen.

▼ So löschen Sie DHCP-Optionen (DHCP Manager)

1. **Wählen Sie in DHCP Manager die Registerkarte „Optionen“.**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

2. **Wählen Sie die Option aus, die Sie löschen möchten.**

3. **Wählen Sie „Löschen“ im Menü „Bearbeiten“ aus.**

   Das Dialogfeld „Option löschen“ wird angezeigt.

4. **Aktivieren Sie das Kontrollkästchen „DHCP-Server von Änderung benachrichtigen“, wenn Sie keine weiteren Optionen mehr löschen möchten.**

   Diese Auswahl weist den DHCP-Server an, die `dhcptab`-Tabelle erneut einzulesen, um die darin vorgenommenen Änderungen unmittelbar nach dem Klicken auf „OK“ zu übernehmen.

5. **Klicken Sie auf „OK“.**

▼ So löschen Sie DHCP-Optionen (`dhtadm`)

1. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Löschen Sie eine DHCP-Option, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

```
# dhtadm -D -s option-name -g
```

Ändern der Optionsinformationen eines Oracle Solaris DHCP-Client

Wenn Sie eine neue DHCP-Option zu Ihrem DHCP-Server hinzufügen, müssen Sie jeder Optionsinformationen des DHCP-Clients einen ergänzenden Eintrag hinzufügen. Bei DHCP-Clients, bei denen es sich nicht um Oracle Solaris DHCP-Clients handelt, suchen Sie in der Dokumentation nach Informationen zum Hinzufügen von Optionen bzw. Symbolen.

Bei einem Oracle Solaris DHCP-Client müssen Sie der Datei `/etc/dhcp/inittab` einen Eintrag für jede Option hinzufügen, die Sie dem DHCP-Server hinzufügen. Wenn Sie die Option später auf dem Server ändern, müssen Sie auch den Eintrag in der `/etc/dhcp/inittab`-Clientdatei bearbeiten.

Ausführliche Informationen zur Syntax der `/etc/dhcp/inittab`-Datei finden Sie in der Manpage `dhcp_inittab(4)`.

Hinweis – Haben Sie der `dhcptags`-Datei in einer früheren Oracle Solaris-Version DHCP-Optionen hinzugefügt, so müssen Sie diese Optionen auch der `/etc/dhcp/inittab`-Datei hinzufügen. Weitere Informationen finden Sie unter „DHCP-Optionsinformationen“ auf Seite 506.

Unterstützung der Oracle Solaris-Netzwerkinstallation mit dem DHCP-Service

Mit DHCP können Sie Oracle Solaris auf bestimmten Clientsystemen in Ihrem Netzwerk installieren. Diese Funktion kann jedoch nur für `sun4u`-basierte Systeme und x86-Systeme verwendet werden, die die Hardwareanforderungen zur Ausführung von Oracle Solaris erfüllen. Informationen zum Verwenden von DHCP zur automatischen Konfiguration von Clientsystemen für das Netzwerk während des Bootens finden Sie in Kapitel 2, „Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)" in *Oracle Solaris 10 9/10 Installationshandbuch: Netzwerkbasierte Installation*.

Darüber hinaus unterstützt DHCP Oracle Solaris-Clientsysteme, die unter Verwendung von HTTP standortfern von Servern über ein WAN gebootet und installiert werden. Diese Methode des Remote-Bootens und der Remote-Installation wird als *WAN-Boot-Installation* bezeichnet. Mithilfe von WAN-Boot können Sie Oracle Solaris auch dann über ein großes öffentliches Netzwerk auf SPARC-basierten Systemen installieren, wenn die Netzwerk-Infrastruktur nicht vertrauenswürdig erscheint. Die Sicherheitsfunktionen von WAN-Boot schützen die Vertraulichkeit der Daten und stellen die Integrität des Installationsabbilds sicher.

Bevor Sie DHCP zum remoten Booten und zur remoten Installation von Clientsystemen mithilfe von WAN-Boot verwenden können, muss der DHCP-Server so konfiguriert werden, dass er den Clients die folgenden Informationen bereitstellt:

- Die IP-Adresse des Proxy-Servers
- Den Speicherort des `wanboot–cgi`-Programms

Ausführliche Informationen zur Konfiguration des DHCP-Servers zur Bereitstellung dieser Informationen finden Sie in Kapitel 2, „Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)" in *Oracle Solaris 10 9/10 Installationshandbuch: Netzwerkbasierte Installation*. Informationen zum Booten und zur Installation von Clientsystemen mit einem DHCP-Server über ein WAN finden Sie in Kapitel 10, „WAN-Boot (Übersicht)" in *Oracle Solaris 10 9/10 Installationshandbuch: Netzwerkbasierte Installation*.

Informationen zur Unterstützung von laufwerkslosen Clients finden Sie unter „Unterstützung von remten Booten und laufwerkslosen Boot-Clients (Übersicht der Schritte)" auf Seite 440.

Unterstützung von remten Booten und laufwerkslosen Boot-Clients (Übersicht der Schritte)

Der Oracle Solaris DHCP-Service kann Oracle Solaris-Clientsysteme unterstützen, die ihre Betriebssystemdateien remote von einem anderen Computer (dem Betriebssystemserver) aus

einhängen. Solche Clients werden häufig als *laufwerkslose Clients* bezeichnet. Laufwerkslose Clients kann man sich als Clients vorstellen, die ständig standortfern booten. Jedes Mal, wenn ein laufwerksloser Client bootet, muss der Client den Namen und die IP-Adresse des Servers beziehen, auf dem die Betriebssystemdateien des Hosts gespeichert sind. Erst dann kann der laufwerkslose Client remote von diesen Dateien gebootet werden.

Jeder laufwerkslose Client verfügt über eine eigene Root-Partition auf dem Betriebssystemserver, die auf dem Client-Hostnamen freigegeben ist. Der DHCP-Server muss dem laufwerkslosen Client jedes Mal die gleiche IP-Adresse zuweisen. Diese Adresse muss dem gleichen Hostnamen im Namen-Service (z. B. DNS) zugewiesen sein. Wenn ein laufwerksloser Client eine konsistente IP-Adresse empfängt, verwendet der Client einen konsistenten Hostnamen und kann auf seine Root-Partition auf dem Betriebssystemserver zugreifen.

Neben der Bereitstellung von IP-Adresse und Hostname kann der DHCP-Server den Speicherort der Betriebssystemdateien des laufwerkslosen Client angeben. Hierzu müssen Sie jedoch Optionen und Makros erstellen, um die Informationen in einem DHCP-Nachrichtenpaket zu übermitteln.

In der folgenden Tabelle sind die Aufgaben aufgeführt, die Sie zur Unterstützung von laufwerkslosen Clients oder anderen persistenten Remote-Boot-Clients ausführen müssen. Die Tabelle enthält Links zu den Verfahren, in denen die Ausführung der Aufgaben beschrieben wird.

Aufgabe	Beschreibung	Siehe
Einrichten der Betriebssystem-Services auf einem Oracle Solaris-Server.	Erstellen Sie mithilfe des Befehls `smosservice` die Betriebssystemdateien für Clients.	Kapitel 7, „Managing Diskless Clients (Tasks)“ in *System Administration Guide: Basic Administration* Lesen Sie auch die Manpage `smosservice`(1M).
Einrichten des DHCP-Services zur Unterstützung von Netzwerk-Boot-Clients.	Erstellen Sie mit DHCP Manager oder dem Befehl `dhtadm` neue Hersteller-Optionen und -Makros, mit denen der DHCP-Client die Boot-Informationen an die Clients übertragen kann. Falls Sie die Optionen für die Netzwerkkonfiguration von Clients bereits erstellt haben, müssen Sie nur Makros für die Hersteller-Clienttypen der laufwerkslosen Clients erstellen.	Kapitel 2, „Vorkonfigurieren der Systemkonfigurationsinformationen (Vorgehen)“ in *Oracle Solaris 10 9/10 Installationshandbuch: Netzwerkbasierte Installation*

Aufgabe	Beschreibung	Siehe
Zuweisen von reservierten IP-Adressen zu den laufwerkslosen Clients.	Kennzeichnen Sie eine IP-Adresse mit DHCP Manager als reserviert, oder verwenden Sie den Befehl `pntadm`, um Adressen für laufwerkslose Clients als `MANUAL` zu kennzeichnen.	„Zuweisen einer reservierten IP-Adresse zu einem DHCP-Client" auf Seite 416
Einrichten von laufwerkslosen Clients für Betriebssystem-Services.	Fügen Sie mit dem Befehl `smdiskless` eine Betriebssystemunterstützung für jeden Client auf dem Betriebssystemserver hinzu. Geben Sie die IP-Adressen an, die Sie für jeden Client reserviert haben.	Kapitel 7, „Managing Diskless Clients (Tasks)" in *System Administration Guide: Basic Administration* Lesen Sie auch die Manpage `smdiskless`(1M).

Einrichten von DHCP-Clients ausschließlich zum Empfang von Informationen (Übersicht der Schritte)

In einigen Netzwerken soll der DHCP-Service den Clients nur Konfigurationsinformationen bereitstellen. Clientsysteme, die Informationen und keine Leasings benötigen, können über den DHCP-Client eine `INFORM`-Nachricht ausgeben. Die `INFORM`-Nachricht fordert den DHCP-Server auf, die entsprechenden Konfigurationsinformationen an den Client zu senden.

Sie können den Oracle Solaris DHCP-Server so einrichten, dass er Clients ausschließlich mit Konfigurationsinformationen unterstützt. Dazu erstellen Sie eine leere Netzwerktabelle, die dem Netzwerk entspricht, das als Host für die Clients auftritt. Die Tabelle muss vorhanden sein, so dass der DHCP-Server auf Clients aus diesem Netzwerk reagieren kann.

In der folgenden Tabelle sind die Aufgaben aufgeführt, die zur Unterstützung von Clients ausschließlich mit Konfigurationsinformationen ausgeführt werden müssen. Die Tabelle enthält Links zu den Verfahren, in denen die Ausführung der Aufgaben beschrieben wird.

Aufgabe	Beschreibung	Siehe
Erstellen einer leeren Netzwerktabelle.	Erstellen Sie mithilfe von DHCP Manager oder den Befehl `pntadm` eine Netzwerktabelle für das Netzwerk der Clients, die nur Konfigurationsinformationen benötigen.	„Hinzufügen von DHCP-Netzwerken" auf Seite 391
Erstellen von Makros, in denen die Informationen enthalten sind, die von den Clients benötigt werden.	Erstellen Sie mithilfe von DHCP Manager oder den Befehl `dhtadm` Makros, um die erforderlichen Informationen an die Clients zu übergeben.	„Erstellen von DHCP-Makros" auf Seite 426

Aufgabe	Beschreibung	Siehe
Ausgeben einer INFORM-Nachricht durch einen DHCP-Client.	Sorgen Sie mit dem Befehl `ifconfig` *int* `dhcp inform` dafür, dass der DHCP-Client eine INFORM-Nachricht ausgibt.	„Start eines DHCP-Clients“ auf Seite 458 „`ifconfig`-Befehlsoptionen für den DHCP-Client“ auf Seite 464 `ifconfig`(1M)-Manpage

Umwandeln des DHCP-Datenspeicherstyps

Oracle Solaris DHCP bietet einen Dienstprogramm, mit dem Sie die DHCP-Konfigurationsdaten von einem Datenspeichertyp in einen anderen Datenspeichertyp umwandeln können. Zum Umwandeln des Datenspeichertyps kann es verschiedene Gründe geben. Vielleicht haben Sie mehr DHCP-Clients, benötigen eine höhere Performance oder eine größere Kapazität vom DHCP-Service, oder Sie möchten Sie die Aufgaben des DHCP-Servers unter mehreren Servern aufteilen. Einen Vergleich der Vor- und Nachteile jedes Datenspeichertyp finden Sie unter „Auswählen des DHCP-Datenspeichers“ auf Seite 343.

Hinweis – Wenn Sie eine Oracle Solaris-Version vor Solaris 8 7/01 aktualisieren, sollten Sie den folgenden Hinweis lesen.

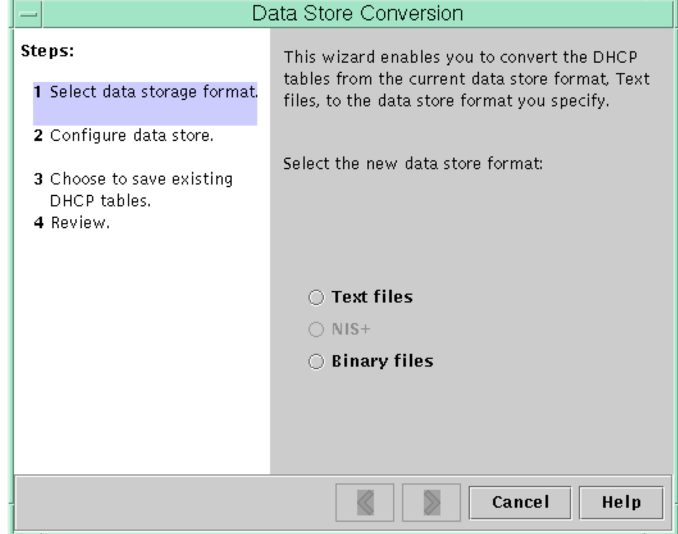
Wenn Sie ein Oracle Solaris DHCP-Tool nach der Installation von Oracle Solaris ausführen, werden Sie aufgefordert, den Datenspeichertyp zu konvertieren. Die Konvertierung wird erforderlich, weil das Format der sowohl in den Dateien als auch im NIS+ gespeicherten Daten im Release Solaris 8 7/01 geändert wurde. Wenn Sie die Konvertierung des Datenspeichertyps nicht vornehmen, liest der DHCP-Server weiterhin die alten Datentabellen ein. Der Server kann jedoch nur Leasings für vorhandene Clients verlängern. Sie können keine neuen DHCP-Clients registrieren oder DHCP-Verwaltungstools mit alten Datentabellen verwenden.

Das Konvertierungsprogramm eignet sich für Standorte, die von einem Sun-Datenspeichertyp zu einem Drittanbieter-Datenspeichertyp konvertieren. Das Konvertierungsprogramm sucht Einträge im vorhandenen Datenspeicher und fügt neue Einträge mit den gleichen Daten in den neuen Datenspeicher ein. Der Datenspeicherzugriff wird mithilfe von separaten Modulen für jeden Datenspeicher umgesetzt. Aufgrund dieses modularen Ansatzes kann das Konvertierungsprogramm DHCP-Daten einem beliebigen Datenspeicherformat in ein beliebiges anderes Datenspeicherformat umwandeln. Jeder Datenspeicher muss über ein Modul verfügen, das der DHCP-Service verwenden kann. Weitere Informationen zum Schreiben eines Moduls zur Unterstützung eines Drittanbieter-Datenspeichers finden Sie in *Solaris DHCP Service Developer's Guide* .

Die Datenspeicherkonvertierung kann in DHCP Manager über den Datenspeicher-Konvertierungsassistenten oder mit dem Befehl `dhcpconfig -C` durchgeführt werden.

In der folgenden Abbildung wird das erste Dialogfeld im Datenspeicher-Konvertierungsassistenten gezeigt.

ABBILDUNG 15–19 Dialogfeld „Datenspeicher-Konvertierung“ in DHCP Manager



Bevor Sie die Konvertierung beginnen, müssen Sie angeben, ob die alten Datenspeichertabellen (`dhcptab` und Netzwerktabellen) gespeichert werden sollen. Dann hält das Konvertierungsprogramm den DHCP-Server an, konvertiert den Datenspeicher, und startet den Server neu, nachdem die Konvertierung erfolgreich abgeschlossen wurde. Wenn Sie das Speichern der alten Tabellen nicht angeben, löscht das Dienstprogramm die Tabellen, nachdem die Konvertierung erfolgreich abgeschlossen wurde. Die Konvertierung kann einige Zeit in Anspruch nehmen. Die Konvertierung wird im Hintergrund ausgeführt und zeigt eine Fortschrittleiste an, die Sie über den Status informiert.

▼ So konvertieren Sie den DHCP-Datenspeicher (DHCP Manager)

1 Wählen Sie in DHCP Manager die Option „Datenspeicher konvertieren“ im Menü „Service“ aus.

Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

Der Datenspeicher-Konvertierungsassistent wird angezeigt.

2 Beantworten Sie die Eingabeaufforderungen des Assistenten.

Wenn Sie Probleme haben, die angeforderten Informationen anzugeben, klicken Sie auf „Hilfe", um ausführliche Informationen zu jedem Dialogfeld anzuzeigen.

3 Prüfen Sie Ihrer Auswahl und klicken Sie dann auf „Fertig stellen", um die Datenspeicherkonvertierung zu starten.

Der DHCP-Server wird nach Abschluss der Konvertierung neu gestartet. Der Server verwendet unmittelbar den neuen Datenspeicher.

▼ So konvertieren Sie den DHCP-Datenspeicher (`dhcpconfig -C`)

1 Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.

Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Konvertieren Sie den Datenspeicher, indem Sie einen Befehl mit der folgenden Syntax eingeben:

`# /usr/sbin/dhcpconfig -C -r` *resource* `-p` *path*

Ressource	ist der neue Datenspeichertyp, z. B. `SUNWbinfiles`
Pfad	ist der Pfad zu den Daten, z. B. `/var/dhcp`

Wenn Sie die ursprünglichen Daten nach der Konvertierung im alten Datenspeicher beibehalten möchten, geben Sie die Option `-k` an. Um beispielsweise Ihren Datenspeicher zu `SUNWbinfiles` zu konvertieren und den alten Datenspeicher zu speichern, geben Sie den folgenden Befehl ein:

```
# /usr/sbin/dhcpconfig -C -r SUNWbinfiles -p /var/dhcp -k
```

Weitere Informationen zum Dienstprogramm `dhcpconfig` finden Sie in der Manpage `dhcpconfig`(1M).

Verschieben von Konfigurationsdaten zwischen DHCP-Servern (Übersicht der Schritte)

Mit DHCP Manager und dem Dienstprogramm `dhcpconfig` können Sie einige oder alle DHCP-Konfigurationsdaten von einem Oracle Solaris DHCP-Server auf einen anderen Server verschieben. Sie können gesamte Netzwerke und alle IP-Adressen, Makros und die den Netzwerken zugeordneten Optionen verschieben. Alternativ können Sie bestimmte IP-Adressen, Makros und Optionen auswählen. Sie können Makros und Optionen auch kopieren, ohne sie vom ersten Server zu löschen.

Das Verschieben von Daten bietet sich an, wenn Sie eine der folgenden Aufgaben ausführen müssen:

- Hinzufügen eines Servers, der einen Teil der DHCP-Aufgaben übernehmen soll.
- Ersetzen des DHCP-Serversystems.
- Ändern des Pfades zum Datenspeicher, während der gleiche Datenspeicher weiterverwendet wird.

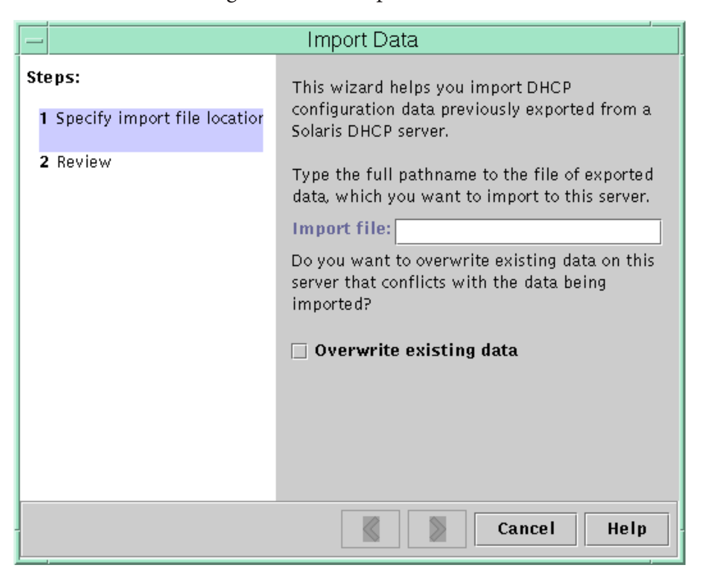
In der folgenden Tabelle sind die Aufgaben aufgeführt, die Sie zum Verschieben der DHCP-Konfigurationsdateien ausführen müssen. Die Tabelle enthält Links zu den Verfahren, in denen die Ausführung der Aufgaben beschrieben wird.

Aufgabe	Beschreibung	Siehe
1. Exportieren der Daten vom ersten Server.	Wählen Sie die Daten aus, die auf einen anderen Server verschoben werden sollen, und erstellen Sie eine Datei der exportierten Daten.	„So exportieren Sie Daten aus einem DHCP-Server (DHCP Manager)“ auf Seite 448 „So exportieren Sie Daten von einem DHCP-Server (`dhcpconfig -X`)“ auf Seite 448
2. Importieren der Daten auf einen zweiten Server.	Kopieren Sie die exportierten Daten in den Datenspeicher eines anderen DHCP-Servers.	„So importieren Sie Daten auf einen DHCP-Server (DHCP Manager)“ auf Seite 450 „So importieren Sie Daten auf einen DHCP-Server (`dhcpconfig -I`)“ auf Seite 450
3. Ändern der importierten Daten für die neue Serverumgebung.	Ändern Sie die Server spezifischen Konfigurationsdateien, damit sie den Informationen des neuen Servers entsprechen.	„So ändern Sie die importierten DHCP-Daten (DHCP Manager)“ auf Seite 451 „So ändern Sie importierte DHCP-Daten (`pntadm`, `dhtadm`)“ auf Seite 452

In DHCP Manager verwenden Sie den „Daten exportieren“-Assistenten und den „Daten importieren“-Assistenten, um die Daten von einem Server auf den anderen zu verschieben. Dann ändern Sie die Makros auf der Registerkarte „Makros“. Die folgenden Abbildungen zeigen die ersten Dialogfelder in den Assistenten.

ABBILDUNG 15–20 Dialogfeld „Daten exportieren“-Assistenten in DHCP Manager

ABBILDUNG 15–21 Dialogfeld „Daten importieren“-Assistenten in DHCP Manager



▼ So exportieren Sie Daten aus einem DHCP-Server (DHCP Manager)

1. **Starten Sie DHCP Manager auf dem Server, von dem Sie Daten verschieben oder kopieren möchten.**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager“ auf Seite 370.

2. **Wählen Sie die Option „Daten exportieren“ im Menü „Service“ aus.**

   Der Assistent „Daten exportieren“ wird angezeigt. Siehe Abbildung 15–20.

3. **Beantworten Sie die Eingabeaufforderungen des Assistenten.**

   Falls Probleme auftreten, klicken Sie auf „Hilfe“, um ausführliche Informationen zu den Eingabeaufforderungen anzuzeigen.

4. **Verschieben Sie die Exportdatei an einen Speicherort, auf den der DHCP-Server, der die Daten importieren muss, zugreifen kann.**

Siehe auch Importieren Sie die Daten gemäß der Beschreibung unter „So importieren Sie Daten auf einen DHCP-Server (DHCP Manager)“ auf Seite 450.

▼ So exportieren Sie Daten von einem DHCP-Server (`dhcpconfig -X`)

1. **Melden Sie sich bei dem Server an, von dem Sie Daten verschieben oder kopieren möchten.**

2. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

3 Exportieren Sie die Daten.

Sie können entweder alle DHCP-Daten oder nur bestimmte Datenteile exportieren.

- **Um nur bestimmte Adressen, Makros und Optionen zu exportieren, geben Sie einen Befehl mit der folgenden Syntax ein:**

  `# dhcpconfig -X` *filename* `-a` *network-addresses* `-m` *macros* `-o` *options*

  Dateiname ist der vollständige Pfadname, den Sie zum Speichern der komprimierten exportierten Daten verwenden möchten. Sie können bestimmte Netzwerkadressen, DHCP-Makros und DHCP-Optionen in durch Kommata getrennten Listen angeben. Das folgende Beispiel zeigt, wie bestimmte Netzwerke, Makros und Optionen exportiert werden.

  ```
  # dhcpconfig -X /var/dhcp/0dhcp1065_data \
  -a 10.63.0.0,10.62.0.0 \
  -m 10.63.0.0,10.62.0.0,SUNW.Sun-Blade-100 -o Sterm
  ```

- **Zum Exportieren aller DHCP-Daten geben Sie einen Befehl mit dem Schlüsselwort `ALL` ein.**

  `# dhcpconfig -X` *filename* `-a ALL -m ALL -o ALL`

  Dateiname ist der vollständige Pfadname, den Sie zum Speichern der komprimierten exportierten Daten verwenden möchten. Das Schlüsselwort `ALL` kann mit den Befehlsoptionen verwendet werden, um alle Netzwerkadressen, Makros oder Optionen zu exportieren. Das folgende Beispiel zeigt, wie Sie den Befehl `ALL` verwenden.

  ```
  # dhcpconfig -X /var/dhcp/dhcp1065_data -a ALL -m ALL -o ALL
  ```

Tipp – Sie können den Export bestimmter Dateien verhindern, indem Sie die `dhcpconfig`-Befehlsoptionen für diesen Datentyp weglassen. Wenn Sie beispielsweise die Option `-m` nicht mit angeben, werden keine DHCP-Makros exportiert.

Weitere Informationen zum Befehl `dhcpconfig` finden Sie in der Manpage `dhcpconfig`(1M).

4 Verschieben Sie die Exportdatei an einen Speicherort, auf den der DHCP-Server, der die Daten importieren soll, zugreifen kann.

Siehe auch Importieren Sie die Daten gemäß der Beschreibung unter „So importieren Sie Daten auf einen DHCP-Server (`dhcpconfig -I`)“ auf Seite 450.

▼ So importieren Sie Daten auf einen DHCP-Server (DHCP Manager)

1. **Starten Sie DHCP Manager auf dem Server, auf den Sie die Daten verschieben möchten, die Sie zuvor von einem anderen DHCP-Server exportiert haben.**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Wählen Sie die Option „Daten importieren" im Menü „Service" aus.**

   Der Assistent „Daten importieren" wird angezeigt. Siehe Abbildung 15–21.

3. **Beantworten Sie die Eingabeaufforderungen des Assistenten.**

   Falls Probleme auftreten, klicken Sie auf „Hilfe", um ausführliche Informationen zu den Eingabeaufforderungen anzuzeigen.

4. **Falls erforderlich, ändern Sie die importierten Daten.**

   Lesen Sie dazu „So ändern Sie die importierten DHCP-Daten (DHCP Manager)" auf Seite 451

▼ So importieren Sie Daten auf einen DHCP-Server (`dhcpconfig -I`)

1. **Melden Sie sich bei dem Server an, auf den Sie die Daten importieren möchten.**

2. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle" auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

3. **Importieren Sie die Daten, indem Sie einen Befehl mit der folgenden Syntax eingeben:**

   `#` **`dhcpconfig -I`** *filename*

   Dateiname ist der Name der Datei, in der die exportierten Daten enthalten sind.

4. **Falls erforderlich, ändern Sie die importierten Daten.**

   Lesen Sie dazu „So ändern Sie importierte DHCP-Daten (`pntadm`, `dhtadm`)" auf Seite 452.

▼ So ändern Sie die importierten DHCP-Daten (DHCP Manager)

1. **Starten Sie DHCP Manager auf dem Server, auf dem Sie Daten importiert haben.**

   Weitere Informationen zu DHCP-Manager finden Sie unter „So starten und stoppen Sie DHCP Manager" auf Seite 370.

2. **Prüfen Sie die importierten Daten auf Netzwerk-spezifische Informationen, die geändert werden müssen.**

   Angenommen, Sie haben Netzwerke verschoben, so müssen Sie die Registerkarte „Adressen" öffnen und den Eigner-Server der Adressen in den importierten Netzwerken ändern. Eventuell müssen Sie auch die Registerkarte „Makros" öffnen, um in einigen Makros die richtigen Domänennamen für NIS, NIS+ oder DNS anzugeben.

3. **Öffnen Sie die Registerkarte „Adressen" und wählen Sie eines der importierten Netzwerke aus.**

4. **Um alle Adressen auszuwählen, klicken Sie auf die erste Adresse, drücken und halten die Umschalttaste gedrückt und klicken dann auf die letzte Adresse.**

5. **Wählen Sie „Eigenschaften" im Menü „Bearbeiten" aus.**

   Das Dialogfeld „Mehrere Adressen ändern" wird angezeigt.

6. **Geben Sie den Namen des neuen Servers an der Eingabeaufforderung „Verwaltungs-Server" ein.**

7. **An der Eingabeaufforderung „Konfigurationsmakro" wählen Sie das Makro, das für alle Clients in diesem Netzwerk verwendet werden soll und klicken dann auf „OK".**

8. **Öffnen Sie Registerkarte „Makros".**

9. **Klicken Sie auf die Schaltfläche „Suchen", um die Optionen zu finden, bei denen wahrscheinlich Werte geändert werden müssen.**

   Die Schaltfläche „Suchen" befindet sich unten im Fenster.

   `DNSdmain`, `DNSserv`, `NISservs`, `NIS+serv` und `NISdmain` sind Beispiele für Optionen, die auf dem neuen Server geändert werden müssen.

10. **Ändern Sie die Optionen in den entsprechenden Makros.**

    Informationen zu den Verfahren zum Ändern von Optionen finden Sie unter „So ändern Sie die Eigenschaften einer DHCP-Option (DHCP Manager)" auf Seite 436.

▼ So ändern Sie importierte DHCP-Daten (`pntadm`, `dhtadm`)

1. **Melden Sie sich auf dem Server an, auf dem Sie Daten importiert haben.**

2. **Melden Sie sich als Superuser an, oder nehmen Sie eine Rolle oder einen Benutzernamen an, der bzw. dem das DHCP Management-Profil zugewiesen ist.**

   Weitere Informationen zum DHCP Management-Profil finden Sie unter „Einrichten des Benutzerzugriffs auf DHCP-Befehle“ auf Seite 371.

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

3. **Prüfen Sie die Netzwerktabellen auf Daten, die geändert werden müssen.**

   Wenn Sie Netzwerke verschoben haben, geben Sie den Befehl `pntadm -P` *Netzwerkadresse* ein, um die Netzwerktabellen für die verschobenen Netzwerke auszudrucken.

4. **Ändern Sie die IP-Adressinformationen mithilfe des Befehls `pntadm`.**

   Eventuell müssen Sie den Eigner-Server und das Konfigurationsmakro für die importierten Adressen ändern. Um beispielsweise den Eigner-Server (`10.60.3.4`) und das Makro (`dhcpsrv-1060`) für die Adresse `10.63.0.2` zu ändern, geben Sie den folgenden Befehl ein:

   ```
   pntadm -M 10.63.0.2 -s 10.60.3.4 -m dhcpsrv-1060 10.60.0.0
   ```

   Wenn zahlreiche Adressen involviert sind, sollten Sie eventuell ein Skript erstellen, das Befehle zum Ändern jede Adresse enthält. Führen Sie das Skript mit dem Befehl `pntadm -B` aus, der `pntadm` im Batch-Modus ausführt. Weitere Informationen finden Sie in der Manpage `pntadm`(1M).

5. **Prüfen Sie die `dhcptab`-Makros auf Optionen mit Werten, die geändert werden müssen.**

   Geben Sie den Befehl `dhtadm -P` ein, um die gesamte `dhcptab`-Tabelle auf dem Bildschirm auszugeben. Suchen Sie mit `grep` oder einem anderen Tool nach Optionen oder Werten, die geändert werden müssen.

6. **Ändern Sie die Optionen in den Makros gegebenenfalls mithilfe des Befehls `dhtadm -M`.**

   Eventuell müssen Sie auch einige Makros ändern, um die richtigen Domänennamen und Server für NIS, NIS+ oder DNS anzugeben. Beispielsweise ändert der folgende Befehl die Werte von `DNSdmain` und `DNSserv` in dem Makro `mymacro`:

   ```
   dhtadm -M -m mymacro -e 'DNSserv=dnssrv2:DNSdmain=example.net' -g
   ```

KAPITEL 16

Konfiguration und Verwaltung des DHCP-Clients

In diesem Kapitel wird der Dynamic Host Configuration Protocol (DHCP)-Client beschrieben, der zu Oracle Solaris gehört. In diesem Kapitel wird erklärt, wie die DHCPv4- und DHCPv6-Protokolle des Clients arbeiten, und wie Sie das Verhalten des Clients beeinflussen können.

Ein Protokoll, DHCPv4, ist seit langem Teil von Oracle Solaris. Es ermöglicht, dass DHCP-Server Konfigurationsparameter wie IPv4-Netzwerkadressen an IPv4-Knoten übergeben können.

Das andere Protokoll, DHCPv6, ermöglicht es DHCP-Servern, Konfigurationsinformationen wie z. B. IPv6-Adressen an IPv6-Knoten zu übergeben. DHCPv6 ist das statusbehaftete Gegenstück zur „IPv6 Stateless Address Autoconfiguration“ (RFC 2462), kann separat oder gleichzeitig mit dem statusfreien Protokoll verwendet werden, um Konfigurationsparameter zu beziehen.

Dieses Kapitel enthält die folgenden Informationen:

- „Allgemeine Informationen zum Oracle Solaris DHCP-Client“ auf Seite 454
- „Aktivieren und Deaktivieren eines Oracle Solaris DHCP-Clients“ auf Seite 462
- „Verwaltung eines DHCP-Client“ auf Seite 463
- „DHCP-Clientsysteme mit mehreren Netzwerkschnittstellen“ auf Seite 466
- „Hostnamen für DHCPv4-Clients“ auf Seite 467
- „DHCP -Clientsysteme und Namen-Services“ auf Seite 468
- „DHCP-Client Ereignisskripten“ auf Seite 473

Allgemeine Informationen zum Oracle Solaris DHCP-Client

Der Oracle Solaris DHCP-Client ist der `dhcpagent`-Daemon, Teil von Oracle Solaris. Wenn Sie Oracle Solaris installieren, werden Sie aufgefordert, DHCP zur Konfiguration der Schnittstellen zu verwenden. Wenn Sie die Frage nach DHCPv4 mit ?Ja" beantworten, wird das Protokoll während der Oracle Solaris-Installation auf Ihrem System aktiviert. Während der Installation können keine Optionen für DHCPv6 angegeben werden. Eine entsprechende Frage bezieht sich jedoch auf IPv6. Wenn Sie IPv6 aktivieren, wird auch DHCPv6 in einem lokalen Netzwerk aktiviert, dass DHCPv6 unterstützt.

Bei einem Oracle Solaris-Client, der DHCP verwendet, sind keine weiteren Schritte erforderlich. Die Konfiguration des DHCP-Servers legt fest, welche Informationen an DHCP-Clientsysteme übergeben werden, die den DHCP-Service verwenden.

Wenn ein Clientsystem Oracle Solaris ausführt, DHCP aber noch nicht verwendet, können Sie das Clientsystem zur Verwendung von DHCP neukonfigurieren. Entsprechend können Sie ein DHCP-Clientsystem neu konfigurieren, so dass es nicht mehr DHCP und stattdessen die von Ihnen bereitgestellten statischen Netzwerkinformationen verwendet. Weitere Informationen finden Sie unter „Aktivieren und Deaktivieren eines Oracle Solaris DHCP-Clients" auf Seite 462.

DHCPv6-Server

Sun Microsystems stellt keinen DHCPv6-Server für Oracle Solaris zur Verfügung. Die von Drittanbietern angebotenen Server sind mit Suns DHCPv6 kompatibel. Wenn ein DHCPv6-Server im Netzwerk verfügbar ist, wird er von Suns DHCPv6-Client verwendet.

Weitere Informationen zum DHCPv4-Server von Sun finden Sie unter „Oracle Solaris DHCP-Server" auf Seite 326.

Unterschiede zwischen DHCPv4 und DHCPv6

Die beiden wesentlichen Unterschiede zwischen DHCPv4 und DHCPv6 sind:

- **Das administrative Modell**
  - DHCPv4 – Der Administrator aktiviert DHCP für jede Schnittstelle. Die Administration erfolgt pro logischer Schnittstelle.
  - DHCPv6 – Eine explizite Konfiguration ist nicht erforderlich. Dieses Protokoll wird auf einer angegebenen physikalischen Schnittstelle aktiviert.
- **Protokolldetails**
  - DHCPv4 – Der DHCP-Server stellt die Teilnetzmaske für jede Adresse bereit. Eine Hostname-Option stellt den systemweit geltenden Knotennamen ein.

- DHCPv6 – Die Teilnetzmaske wird über Router-Advertisement-Nachrichten bekannt gegeben, nicht vom DHCPv6-Server. Es gibt keine Hostname-Option für DHCPv6.

Das administrative Modell

DHCPv4 erfordert die explizite Konfiguration von Clients. Falls die Adressierung gewünscht wird, müssen Sie das DHCPv4-System dazu einrichten. Dies erfolgt in der Regel während der Erstinstallation oder dynamisch mithilfe von `ifconfig(1M)`-Optionen.

DHCPv6 erfordert keine explizite Konfiguration des Clients. Stattdessen ist der Einsatz von DHCP eine Eigenschaft des Netzwerks, und das Signal zum Verwenden von DHCP wird in Router-Advertisement-Nachrichten von lokalen Routern gesendet. Der DHCP-Client erstellt und löscht logische Schnittstellen je nach Bedarf.

Bei der Verwaltung ähnelt der DHCPv6 -Mechanismus der bereits bestehenden IPv6-statusfreien (automatischen) Adresskonfiguration. Bei der statusfreien Adresskonfiguration richten Sie ein Flag für den lokalen Router ein, dass jeder Client in einem bestimmten Präfixbereich automatisch selbst eine Adresse erzeugen soll. Dazu verwendet er das bekannt gegebene Präfix plus ein lokales Schnittstellentoken oder eine Zufallszahl. Für DHCPv6 sind die gleichen Präfixe erforderlich, aber die Adressen werden über einen DHCPv6-Server erhalten und verwaltet und nicht „zufällig zugewiesen."

MAC-Adresse und Client-ID

DHCPv4 verwendet die MAC-Adresse und eine optionale Client-ID, um den Client zu erkennen, so dass ihm eine Adresse zugewiesen werden kann. Jedes Mal, wenn der gleiche Client im Netzwerk eintrifft, erhält er, sofern möglich, die gleiche Adresse.

DHCPv6 verwendet grundsätzlich das gleiche Schema, aber die Client-ID ist obligatorisch und bildet die Grundlage für die Adressstruktur. Die Client-ID in DHCPv6 besteht aus zwei Komponenten: einem DHCP Unique Identifier (DUID) und einem Identity Association Identifier (IAID). Die DUID kennzeichnet das Client**system** (und nicht nur eine Schnittstelle wie bei DHCPv4), und die IAID kennzeichnet die Schnittstelle auf diesem System.

Wie in RFC 3315 beschrieben, wird eine Identity Association für einen Server und einen Client verwendet, um einen Satz verwandter IPv6-Adressen zu identifizieren, zu gruppieren und zu verwalten. Ein Client muss jeder seiner Netzwerkschnittstellen mindestens eine bestimmte IA zuordnen. Dann verwendet er die zugeordneten IAs, um die Konfigurationsinformationen für diese Schnittstelle von einem Server zu beziehen. Weitere Informationen zu IAs finden Sie im folgenden Abschnitt „Protokolldetails."

DUID+IAID können zusammen mit DHCPv4 verwendet werden. Sie werden unverwechselbar miteinander verkettet, so dass sie als die Client-ID verwendet werden können. Aus Kompatibilitätsgründen wird dies für reguläre IPv4-Schnittstellen nicht durchgeführt. Für logische Schnittstellen ("hme0:1") kann DUID+IAID jedoch verwendet werden, wenn keine Client-ID konfiguriert wurde.

Im Gegensatz zu IPv4 DHCP, stellt DHCPv6 keine „Clientname“-Option bereit, so dass es keine Möglichkeit gibt, Ihre Systeme allein basierend auf DHCPv6 zu benennen. Wenn Sie stattdessen den DNS-Namen wissen müssen, der zu einer von DHCPv6 bereitgestellten Adresse gehört, verwenden Sie die DNS Reverse-Resolution (Adresse-zu-Name-Abfrage über die Funktion `getaddrinfo(3SOCKET)`), um die entsprechenden Namensinformationen zu suchen. Der Nachteil dabei: wenn Sie nur DHCPv6 verwenden und möchten, dass ein Knoten einen bestimmten Namen hat, müssen Sie `/etc/nodename` auf Ihrem System einrichten.

Protokolldetails

Bei DHCPv4 stellt der DHCP-Server die Teilnetzmaske bereit, die mit der zugewiesenen Adresse verwendet wird. Bei DHCPv6 wird die Teilnetzmaske (auch als „Präfixlänge“ bezeichnet) durch Router-Advertisement-Nachrichten zugewiesen und nicht vom DHCP-Server gesteuert.

DHCPv4 verfügt über eine Hostname-Option, über die ein systemweit geltender Knotenname eingerichtet werden kann. DHCPv6 bietet eine solche Option nicht.

Um eine Client-ID für DHCPv6 zu konfigurieren, müssen Sie eine DUID angeben. Gestatten Sie dem System nicht, automatisch eine DUID auszuwählen. Sie können dies global für den Daemon oder für jede Schnittstelle einzeln ausführen. Zum Einrichten der globalen DUID verwenden Sie die folgende Syntax (beachten Sie den einleitenden Punkt):

```
.v6.CLIENT_ID=<DUID>
```

Mit dem folgenden Befehl sorgen Sie dafür, dass eine bestimmte Schnittstelle eine angegebene DUID verwendet (und das System gegenüber einem DHCPv6-Server als mehrere unabhängige Clients auftritt):

```
hme0.v6.CLIENT ID=<DUID>
```

Jede Identity Association (IA) enthält einen Adresstyp. Beispielsweise nimmt eine Identity Association für temporäre Adressen (IA_TA) temporäre Adressen auf, während eine Identity Association für nicht-temporäre Adressen (IA_NA) zugewiesene permanente Adressen aufnimmt. Die in diesem Handbuch beschriebene Version von DHCPv6 bietet nur IA_NA-Zuweisungen.

Oracle Solaris weist jeder Schnittstelle auf Anforderung genau eine IAID zu, die in einer Datei im Root-Dateisystem gespeichert wird, so dass sie über die Lebensdauer des Computers konstant bleibt.

Logische Schnittstellen

Bei dem DHCPv4-Client ist jede logische Schnittstelle unabhängig und eine administrative Einheit. Zusätzlich zur nullten logischen Schnittstelle (die standardmäßig die MAC-Adresse der Schnittstelle als Bezeichner verwendet), kann der Benutzer bestimmte logische Schnittstellen zur Ausführung von DHCP konfigurieren, indem er eine CLIENT_ID in der Konfigurationsdatei `dhcpagent` angibt. Beispiel:

```
hme0:1.CLIENT_ID=orangutan
```

DHCPv6 arbeitet anders. Die nullte logische Schnittstelle auf einer IPv6-Schnittstelle ist im Gegensatz zu IPv4 immer Link-lokal. Link-lokal wird verwendet, um einem Gerät in einem IP-Netzwerk automatisch eine IP-Adresse zuzuweisen, wenn keine andere Zuweisungsmethode (z. B. ein DHCP-Server) verfügbar ist. Die nullte logische Schnittstelle kann nicht unter die Verwaltung von DHCP gestellt werden, daher weist sie, obwohl DHCPv6 auf der nullten logischen Schnittstelle ausgeführt wird (auch als „physikalische“ Schnittstelle bezeichnet), nur logischen Schnittstellen, die nicht null sind, Adressen zu.

Als Antwort auf eine DHCPv6-Client-Anforderung gibt der DHCPv6-Server eine Adressenliste an den zu konfigurierenden Client zurück.

Optionsaushandlung

In DHCPv6 gibt es eine Option „Optionsanforderungen“, die dem Server einen Hinweis bietet, was der Client sehen möchte. Wenn der Server alle möglichen Optionen an den Client sendet, könnten so viele Informationen gesendet werden, dass sie auf dem Weg zum Client eventuell abgeworfen werden. Der Server kann basierend auf diesem Hinweis Optionen auswählen, die in die Antwort aufgenommen werden. Alternativ kann der Server den Hinweis ignorieren und andere Objekte auswählen, die an den Client gesendet werden. Unter Oracle Solaris würden die bevorzugten Optionen z. B. die Oracle Solaris DNS-Adressdomäne oder die NIS-Adressdomäne enthalten, den NetBios-Server jedoch nicht.

Der gleiche Hinweistyp wird auch für DHCPv4 angeboten, jedoch ohne die spezielle Option zur Optionsanforderung. Stattdessen verwendet DHCPv4 `PARAM_REQUEST_LIST` in `/etc/default/dhcpagent`.

Konfigurationssyntax

Sie konfigurieren den DHCPv6-Client auf nahezu die gleiche Weise wie einen bestehenden DHCPv4-Client: mithilfe von `/etc/default/dhcpagent`.

Die Syntax wird mit dem Kennzeichen „v6” zwischen dem Schnittstellennamen (falls vorhanden) und dem zu konfigurierenden Parameter erweitert. Die globale Liste zur IPv4-Optionsanforderung sieht wie folgt aus:

```
PARAM_REQUEST_LIST=1,3,6,12,15,28,43
```

Eine einzelne Schnittstelle kann so konfiguriert werden, dass die Hostname-Option weggelassen wird:

```
hme0.PARAM_REQUEST_LIST=1,3,6,15,28,43
```

Zum Einrichten einer globalen Anforderungsliste für DHCPv6 verwenden Sie den folgenden Befehl (beachten Sie den einleitenden Punkt):

```
.v6.PARAM_REQUEST_LIST=23,24
```

Oder richten Sie, wie in dem folgenden Beispiel, eine einzelne Schnittstelle ein:

```
hme0.v6.PARAM_REQUEST_LIST=21,22,23,24
```

Zur Referenz eine tatsächliche `/etc/default/dhcpagent`-Datei für die DHCPv6-Konfiguration:

```
# The default DHCPv6 parameter request list has preference (7), unicast (12),
# DNS addresses (23), DNS search list (24), NIS addresses (27), and
# NIS domain (29).  This may be changed by altering the following parameter-
# value pair.  The numbers correspond to the values defined in RFC 3315 and
# the IANA dhcpv6-parameters registry.
.v6.PARAM_REQUEST_LIST=7,12,23,24,27,29
```

Start eines DHCP-Clients

In den meisten Fällen müssen Sie beim Start eines DHCPv6-Clients nichts ausführen. Der `in.ndpd`-Daemon startet DHCPv6 gegebenenfalls automatisch. Es kann sein, dass Sie für `/etc/hostname6.$IFNAME` eine Touch-Operation durchführen müssen, um eine Schnittstelle zu konfigurieren, die zur Boot-Zeit für IPv6 geplumbt werden soll. Dies übernimmt jedoch das Installationsprogramm für Sie, wenn Sie IPv6 während der Installation auf Ihrem System aktiviert haben.

Bei DHCPv4 müssen Sie den Start des Clients jedoch anfordern, falls dies nicht während der Oracle Solaris-Installation erfolgt ist. Weitere Informationen finden Sie unter „So aktivieren Sie den Oracle Solaris DHCP-Client" auf Seite 462.

Der `dhcpagent`-Daemon bezieht Konfigurationsinformationen, die von anderen, am Boot-Vorgang des Systems beteiligten Prozessen benötigt werden. Aus diesem Grund startet das System-Startskript den `dhcpagent`-Daemon bereits sehr früh im Boot-Vorgang und wartet, bis die Netzwerkkonfigurationsinformationen vom DHCP-Server eintreffen.

Obwohl DHCPv6 standardmäßig ausgeführt wird, können Sie wählen, DHCPv6 nicht auszuführen. Wenn DHCPv6 bereits ausgeführt wird, können Sie es mit dem Befehl `ifconfig` stoppen. Sie können DHCPv6 auch deaktivieren, so dass es bei einem erneuten Booten nicht mehr ausgeführt wird. Dazu nehmen Sie Änderungen an der`/etc/inet/ndpd.conf`-Datei vor.

Mit dem folgenden Code fahren Sie beispielsweise DHCPv6 auf einer Schnittstelle namens „hme0“ herunter.”

```
ex# echo ifdefault StatefulAddrConf false >> /etc/inet/ndpd.conf
ex# pkill -HUP -x in.ndpd
ex# ifconfig hme0 inet6 dhcp release
```

Das Vorhandensein der Datei `/etc/dhcp.`*Schnittstelle* (z. B. `/etc/dhcp.ce0` auf einem Sun Fire 880-System) weist die Startskripten an, DHCPv4 auf einer bestimmten Schnittstelle zu verwenden. Sobald eine `dhcp.`*Schnittstelle*-Datei gefunden wurde, startet das Startskript den `dhcpagent`-Daemon.

Nach dem Start wartet `dhcpagent`, bis er Anweisungen zur Konfiguration einer Netzwerkschnittstelle empfängt. Die Startskripten geben den Befehl `ifconfig` *Schnittstelle* `dhcp start` aus, der `dhcpagent` anweist, DHCPv4 gemäß der Beschreibung unter „Arbeitsweise des DHCP-Protokolls“ auf Seite 323 zu starten. Eventuell in der `dhcp.`*Schnittstelle*-Datei enthaltene Befehle werden an die `dhcp start`-Option von `ifconfig` angehängt. Weitere Informationen zu Optionen für den Befehl `ifconfig` *Schnittstelle* `dhcp` finden Sie in der Manpage `ifconfig`(1M).

DHCPv6-Kommunikation

Im Gegensatz zu DHCPv4, das durch manuelle Konfiguration aufgerufen wird, erfolgt der Aufruf von DHCPv6 durch Router Advertisement-Nachrichten (RAs). Abhängig von der Konfiguration des Routers ruft das System DHCPv6 automatisch auf der Schnittstelle auf, auf der die Router Advertisement-Nachricht empfangen wurde und verwendet DHCP, um eine Adresse und andere Parameter zu beziehen. Eventuell fordert das System auch nur andere Daten als eine Adresse (z. B. DNS-Server) mit DHCPv6 an.

Der `in.ndpd`-Daemon empfängt die Router Advertisement-Nachricht. Dies erfolgt automatisch auf allen für IPv6 beim System geplumbten Schnittstellen. Wenn `in.ndpd` eine RA sieht, in der angegeben ist, dass DHCPv6 ausgeführt werden soll, wird es aufgerufen.

Um zu verhindern, dass `in.ndpd` DHCPv6 startet, können Sie Änderungen an der `/etc/inet/ndpd.conf`-Datei vornehmen.

Sie können DHCPv6 auch nach dem Starten einer der folgenden Versionen von `ifconfig` stoppen:

```
ifconfig <Schnittstelle> inet6 dhcp drop
```

oder:

```
ifconfig <Schnittstelle> inet6 dhcp release
```

So verwalten die DHCP-Client-Protokolle Netzwerkkonfigurationsinformationen

DHCPv4- und DHCPv6-Client-Protokolle verwalten die Netzwerkkonfigurationsinformationen auf unterschiedliche Art. Der wesentliche Unterschied besteht darin, dass bei DHCPv4 die Aushandlung für das Leasing einer einzelnen Adresse und einiger zugehöriger Optionen erfolgt. Bei DHCPv6 erfolgt die Aushandlung für einen Adressstapel und einen Optionsstapel.

Hintergrundinformationen zur Interaktion zwischen DHCPv4-Client und Server finden Sie in Kapitel 12, „Einführung in Oracle Solaris DHCP“.

So verwaltet der DHCPv4-Client Netzwerkkonfigurationsinformationen

Nachdem das Informationspaket von einem DHCP-Server bezogen wurde, konfiguriert der `dhcpagent`-Daemon die Netzwerkschnittstelle und schaltet sie online. Der Daemon steuert die Schnittstelle über die Leasing-Zeit der IP-Adresse und verwaltet die Konfigurationsdaten in einer internen Tabelle. Die System-Startskripten verwenden den Befehl `dhcpinfo`, um die Werte von Konfigurationsoptionen aus der internen Tabelle zu extrahieren. Die Werte werden dann zur Konfiguration des Systems verwendet und ermöglichen dessen Kommunikation im Netzwerk.

Der `dhcpagent`-Daemon wartet passiv, bis ein bestimmter Zeitraum verstrichen ist, in der Regel die Hälfte der Leasing-Zeit. Dann fordert der Daemon eine Verlängerung der Leasing-Zeit von einem DHCP-Server an. Wenn das System `dhcpagent` benachrichtigt, dass die Schnittstelle heruntergefahren oder die IP-Adresse geändert wurde, verwaltet der Daemon die Schnittstelle nicht weiter, bis er erneut vom `ifconfig`-Befehl dazu angewiesen wird. Stellt der `dhcpagent`-Daemon fest, dass die Schnittstelle hochgefahren ist und die IP-Adresse nicht geändert wurde, sendet der Daemon eine Anforderung zur Erneuerung des Leasings an den Server. Kann das Leasing nicht erneuert werden, schaltet der `dhcpagent`-Daemon die Schnittstelle am Ende der Leasing-Zeit offline.

Jedes Mal, wenn `dhcpagent` eine Aktion im Zusammenhang mit dem Leasing durchführt, sucht der Daemon nach einer ausführbaren Datei namens `/etc/dhcp/eventhook`. Wurde eine ausführbare Dateien mit diesem Namen gefunden, wird sie von `dhcpagent` aufgerufen. Weitere Informationen zur Verwendung der ausführbaren Datei für ein Ereignis finden Sie unter „DHCP-Client Ereignisskripten“ auf Seite 473.

So verwaltet der DHCPv6-Client Netzwerkkonfigurationsinformationen

Die DHCPv6-Kommunikation zwischen Client und Server beginnt damit, dass der Client eine Solicitation-Nachricht sendet, um Server zu lokalisieren. Als Antwort senden alle Server, die für

den DHCP-Service zur Verfügung stehen, eine Advertisement-Nachricht. Die Servernachricht enthält mehrere IA_NA (Identity Association Non-Temporary Address)-Datensätze plus weitere Optionen (z. B. DNS-Serveradressen), die der Server bereitstellen kann.

Ein Client kann bestimmte Adressen anfordern (auch mehrere Adresse), indem er seine eigenen IA_NA/IAADDR-Datensätze in der Request-Nachricht einrichtet. In der Regel fordert ein Client bestimmte Adressen an, wenn er alte Adressen aufgezeichnet hat und möchte, dass ihm der Server die gleichen Adressen zur Verfügung stellt (sofern dies möglich ist). Unabhängig davon, was der Client ausführt (auch wenn er keine Adressen anfordert) kann der Server dem Client eine beliebige Anzahl an Adressen für eine einzelne DHCPv6-Transaktion bereitstellen.

Im Folgenden ist ein möglicher Nachrichtendialog zwischen den Clients und Servern aufgeführt.

- Ein Client sendet eine Solicitation-Nachricht, um Server zu lokalisieren.
- Server senden eine Advertisement-Nachricht, um anzugeben, dass sie für DHCP-Services zur Verfügung stehen.
- Ein Client sendet eine Request-Nachricht, um Konfigurationsparameter von Servern mit den höchsten Präferenzwerten anzufordern (einschließlich IP-Adressen). Server-Präferenzwerte werden vom Administrator eingerichtet und reichen von 0 (niedrigste Präferenz) bis 255 (höchste Präferenz).
- Der Server sendet eine Reply-Nachricht mit den Leasing-Zeiten für die Adresse und Konfigurationsdateien.

Wenn der Präferenzwert in der Advertisement-Nachricht 255 beträgt, wählt der DHCPv6-Client diesen Server sofort aus. Wenn der Server mit der höchsten Präferenz nicht reagiert oder keine Antwort auf die Request-Nachricht sendet, sucht der Client weiter nach Servern mit geringerer Präferenz, bis keine Advertisement-Nachrichten mehr vorliegen. Dann beginnt der Client erneut, Solicitation-Nachrichten zu senden.

Der ausgewählte Server sendet eine Reply-Nachricht mit zugewiesenen Adressen und Konfigurationsparametern als Antwort auf eine Solicitation- oder Request-Nachricht.

Herunterfahren eines DHCP-Clients

Beim Herunterfahren sendet der Client eine Release-Nachricht an den Server, der dem Client die Adressen zugewiesen hat, um ihn zu benachrichtigen, dass er eine oder mehrere der zugewiesenen Adresse nicht mehr benötigt. Wenn das DHCPv4-Clientsystem ordnungsgemäß heruntergefahren wird, schreibt `dhcpagent` die aktuellen Konfigurationsinformationen in die Datei `/etc/dhcp/`*Schnittstelle*`.dhc`, oder (bei DHCPv6) in die Datei `/etc/dhcp/`*Schnittstelle*`.dh6`. In der Standardeinstellung wird das Leasing gespeichert und nicht freigegeben, so dass der DHCP-Server nicht weiß, ob die IP-Adresse noch aktiv verwendet wird. Dadurch ist der Client in der Lage, die Adresse beim nächsten Booten leicht wieder zu beziehen. Diese standardmäßige Aktion entspricht dem Befehl `ifconfig <Schnittstelle> dhcp drop`.

Wenn das Leasing in dieser Datei beim erneuten Booten des Systems noch immer gültig ist, sendet `dhcpagent` eine abgekürzte Anforderung zur Verwendung der gleichen IP-Adresse und der gleichen Netzwerkkonfigurationsinformationen. Bei DHCPv4 ist dies die Request-Nachricht. Bei DHCPv6 ist dies die Confirm-Nachricht.

Wenn der DHCP-Server diese Anforderung zulässt, kann `dhcpagent` die Informationen verwenden, die beim Herunterfahren des Systems gespeichert wurden. Wenn der Server dem Client nicht gestattet, die Informationen zu verwenden, initiiert `dhcpagent` die unter „Arbeitsweise des DHCP-Protokolls“ auf Seite 323 beschriebene DHCP-Protokollfolge. Dadurch bezieht der Client neue Netzwerkkonfigurationsinformationen.

Aktivieren und Deaktivieren eines Oracle Solaris DHCP-Clients

Um den DHCP-Client auf einem System zu aktivieren, auf dem Oracle Solaris ausgeführt, DHCP noch nicht verwendet wird, müssen Sie das System zunächst dekonfigurieren. Wenn das System bootet, geben Sie einige Befehle ein, um das System einzurichten und den DHCP-Client zu aktivieren.

Hinweis – Bei vielen Installationen ist es gebräuchlich, wichtige Teile der Infrastruktur mit statischen IP-Adressen anstelle mit DHCP zu konfigurieren. Eine Aufstellung, welche Geräte in Ihrem Netzwerk Clients sein sollen und welche nicht (z. B. Router und bestimmte Server) sprengt jedoch den Umfang dieses Handbuchs.

▼ So aktivieren Sie den Oracle Solaris DHCP-Client

Dieses Verfahren ist nur dann notwendig, wenn DHCPv4 nicht während der Installation von Oracle Solaris aktiviert wurde. Für DHCPv6 ist dieses Verfahren nie notwendig.

1. **Melden Sie sich als Superuser beim Clientsystem an.**

2. **Wenn das System eine Vorkonfiguration anstelle einer in der aktiven Konfiguration verwendet, nehmen Sie die erforderlichen Änderungen an der Datei `sysidcfg` vor. Fügen Sie den Unterschlüssel `dhcp` zum Schlüsselwort `network_interface` in der Datei `sysidcfg` hinzu.**

   Beispiel: `network_interface=hme0 {dhcp}`. Weitere Informationen finden Sie in der Manpage `sysidcfg(4)`.

3. **Dekonfigurieren Sie das System und fahren Sie es herunter.**

   ```
   # sys-unconfig
   ```

   Weitere Informationen zu den Konfigurationsinformationen, die mit diesem Befehl gelöscht werden, finden Sie in der Manpage `sys-unconfig(1M)`.

4. **Booten Sie das System neu, nachdem es vollständig heruntergefahren ist.**

   Wenn das System vorkonfiguriert ist, konfiguriert der Unterschlüssel `dhcp` in der `sysidcfg`-Datei das System so, dass es den DHCP-Client verwendet.

   Ist das System nicht vorkonfiguriert, werden Sie von den `sysidtool`-Programmen beim Booten des Systems zur Eingabe der Konfigurationsinformationen aufgefordert. Weitere Informationen finden Sie in der Manpage `sysidtool`(1M).

5. **Geben Sie „Ja" an, wenn Sie bestätigen sollen, ob DHCP zur Konfiguration der Netzwerkschnittstellen verwendet werden soll.**

▼ So deaktivieren Sie einen Oracle Solaris DHCP-Client

1. **Melden Sie sich als Superuser beim Clientsystem an.**

2. **Wenn Sie eine `sysidcfg`-Datei zur Vorkonfiguration des Systems verwenden, löschen Sie den Unterschlüssel `dhcp` vom Schlüsselwort `network_interface`.**

3. **Dekonfigurieren Sie das System und fahren Sie es herunter.**

   ```
   # sys-unconfig
   ```

   Weitere Informationen zu den Konfigurationsinformationen, die mit diesem Befehl gelöscht werden, finden Sie in der Manpage `sys-unconfig`(1M).

4. **Booten Sie das System neu, nachdem es vollständig heruntergefahren ist.**

   Wenn das System vorkonfiguriert ist, werden Sie nicht zur Eingabe der Konfigurationsinformationen aufgefordert, und der DHCP-Client wird nicht konfiguriert.

   Ist das System nicht vorkonfiguriert, werden Sie von den `sysidtool`-Programmen beim Booten des Systems zur Eingabe der Konfigurationsinformationen aufgefordert. Weitere Informationen finden Sie in der Manpage `sysidtool`(1M).

5. **Geben Sie „Nein" an, wenn Sie bestätigen sollen, ob DHCP zur Konfiguration der Netzwerkschnittstellen verwendet werden soll.**

Verwaltung eines DHCP-Client

Die Software eines Oracle Solaris DHCP-Client erfordert bei normalem Systembetrieb keine Administration. Der `dhcpagent`-Daemon wird beim Booten des Systems automatisch gestartet, handelt Leasings neu aus und stoppt, wenn das System heruntergefahren wird. Sie sollten den `dhcpagent`-Daemon weder manuell starten noch stoppen. Stattdessen können Sie als Superuser auf dem Clientsystem den Befehl `ifconfig` einsetzen, um die Verwaltung der Netzwerkschnittstelle durch den `dhcpagent`-Daemon zu beeinflussen.

`ifconfig`-Befehlsoptionen für den DHCP-Client

In diesem Abschnitt sind die Befehlsoptionen zusammengefasst, die in der Manpage `ifconfig(1M)` ausführlich beschrieben sind. Der einzige Unterschied zwischen der DHCPv4- und der DHCPv6-Version dieser Befehle liegt in dem Schlüsselwort „inet6". Nehmen Sie das Schlüsselwort „inet6" für DHCPv6 auf, aber lassen Sie es beim Ausführen von DHCPv4 weg.

Mit dem `ifconfig`-Befehl können Sie Folgendes ausführen:

- **Starten des DHCP-Client** – Mit dem Befehl `ifconfig` *Schnittstelle* `[inet6] dhcp start` initiieren Sie die Interaktionen zwischen dem `dhcpagent`-Daemon und dem DHCP-Server, um eine IP-Adresse und einen neuen Satz Konfigurationsoptionen zu beziehen. Dieser Befehl eignet sich insbesondere dann, wenn Sie die Informationen ändern möchten, die ein Client unmittelbar verwenden soll, z. B. wenn Sie IP-Adressen hinzufügen oder die Teilnetzmaske ändern.
- **Anfordern nur der Netzwerkkonfigurationsinformationen** – Mit dem Befehl `ifconfig` *Schnittstelle* `[inet6] dhcp inform` sorgen Sie dafür, dass der `dhcpagent`-Daemon eine Anforderung nach Netzwerkkonfigurationsparametern mit Ausnahme der IP-Adresse sendet. Dieser Befehl eignet sich insbesondere dann, wenn die Netzwerkschnittstelle über eine statische IP-Adresse verfügt, das Clientsystem jedoch aktualisierte Netzwerkoptionen benötigt. So verwenden Sie diesen Befehl immer dann, wenn Sie DHCP nicht zur Verwaltung der IP-Adressen, aber zur Konfiguration der Hosts im Netzwerk verwenden möchten.
- **Anfordern einer Leasing-Verlängerung** – Mit dem Befehl `ifconfig` *Schnittstelle* `[inet6] dhcp extend` sendet der `dhcpagent`-Daemon eine Anforderung zur Erneuerung der Leasing-Zeit. Der Client fordert automatisch eine Erneuerung der Leasing-Zeit an. Sie können diesen Befehl verwenden, wenn Sie die Leasing-Zeit ändern und möchten, dass die Clients die neue Leasing-Zeit sofort verwenden und nicht auf den nächsten Versuch zur Leasing-Erneuerung warten.
- **Freigeben der IP-Adresse** – Mit dem Befehl `ifconfig` *Schnittstelle* `[inet6] dhcp release` wird veranlasst, dass der `dhcpagent`-Daemon die Verwaltung der von der Netzwerkschnittstelle verwendeten IP-Adresse abgibt. Die Freigabe der IP-Adresse erfolgt automatisch, wenn die Leasing-Zeit abgelaufen ist. Sie können diesen Befehl auf einem Laptop eingeben, wenn Sie das Netzwerk verlassen und beabsichtigen, das System in einem anderen Netzwerk neu zu starten. Lesen Sie auch die Informationen zur `RELEASE_ON_SIGTERM`-Eigenschaft in der Konfigurationsdatei `/etc/default/dhcpagent`.
- **Abwerfen der IP-Adresse** – Mit dem Befehl `ifconfig` *Schnittstelle* `[inet6] dhcp drop` wird veranlasst, dass der `dhcpagent`-Daemon die Netzwerkschnittstelle offline schaltet, ohne den DHCP-Server zu benachrichtigen. Die Leasing-Zeit wird im Dateisystem zwischengespeichert. Mit diesem Befehl kann ein Client nach einem Neustart wieder die gleiche IP-Adresse erhalten.
- **Anpingen der Netzwerkschnittstelle** – Mit dem Befehl `ifconfig` *Schnittstelle* `[inet6] dhcp ping` können Sie feststellen, ob die Schnittstelle von DHCP verwaltet wird.

- **Anzeigen des DHCP-Konfigurationsstatus der Netzwerkschnittstelle** – Mit dem Befehl `ifconfig` *Schnittstelle* `[inet6] dhcp status` zeigen Sie den aktuellen Status des DHCP-Clients an. Die Anzeige umfasst folgende Informationen:
  - Ob eine IP-Adresse an den Client gebunden ist
  - Die Anzahl der gesendeten, empfangenen und abgewiesenen Anforderungen
  - Ob es sich bei dieser Schnittstelle um die primäre Schnittstelle handelt
  - Zeitangaben, wann die Leasing-Zeit bezogen wurde, wann sie abläuft, wann Erneuerungsversuche gestartet werden sollen

  Beispiel:

```
# ifconfig hme0 dhcp status
Interface  State         Sent  Recv  Declined  Flags
hme0       BOUND            1     1         0   [PRIMARY]
(Began,Expires,Renew)=(08/16/2005 15:27, 08/18/2005 13:31, 08/17/2005 15:24)

# ifconfig hme0 inet6 dhcp status
Interface  State         Sent  Recv  Declined  Flags
hme0       BOUND            1     0         0   [PRIMARY]
(Began,Expires,Renew)=(11/22/2006 20:39, 11/22/2006 20:41, 11/22/2006 20:40)
```

Einrichten der Konfigurationsparameter eines DHCP-Client

Die `/etc/default/dhcpagent`-Datei auf dem Clientsystem enthält einstellbare Parameter für den `dhcpagent`-Daemon. Mit einem Texteditor können Sie verschiedene Parameter ändern, die sich auf den Clientbetrieb auswirken. Die Datei `/etc/default/dhcpagent` ist ausführlich dokumentiert. Weitere Informationen finden Sie sowohl in der Datei als auch in der Manpage `dhcpagent`(1M).

Die Datei `/etc/dhcp.`*Schnittstelle* ist ein weiterer Speicherort, an dem Parameter eingestellt werden, die sich auf den DHCP-Client auswirken. In dieser Datei eingestellten Parameter werden von den System-Startskripten mit dem Befehl `ifconfig` verwendet. Dies betrifft jedoch nur DHCPv4. Es gibt kein DHCPv6-Äquivalent.

Standardmäßig ist der DHCP-Client wie folgt konfiguriert:

Bei DHCPv4

- Das Clientsystem benötigt keinen bestimmten Hostnamen.

  Wenn Sie möchten, dass ein Client einen bestimmten Hostnamen anfordert, lesen Sie „Hostnamen für DHCPv4-Clients“ auf Seite 467.
- Standardmäßige Anforderungen für den Client befinden sich in `/etc/default/dhcpagent` und umfassen DNS-Server, DNS-Domäne und Broadcast-Adresse.

Die Parameterdatei des DHCP-Client kann so eingerichtet werden, dass weitere Informationen im Schlüsselwort `PARAM_REQUEST_LIST` in der `/etc/default/dhcpagent`-Datei angefordert werden. Der DHCP-Server kann so konfiguriert werden, dass er Optionen bereitstellt, die nicht explizit angefordert wurden. Informationen zur Verwendung von DHCP-Servermakros zum Senden von Informationen an Clients finden Sie unter „Einführung in DHCP-Makros“ auf Seite 334 und „Arbeiten mit DHCP-Makros (Übersicht der Schritte)“ auf Seite 419.

Bei DHCPv4 und DHCPv6

- Das Clientsystem verwendet DHCP auf einer physikalischen Netzwerkschnittstelle.

  Wenn Sie DHCP auf mehreren physikalischen Schnittstellen verwenden möchten, lesen Sie „DHCP-Clientsysteme mit mehreren Netzwerkschnittstellen“ auf Seite 466.
- Der Client wird nicht automatisch als Namen-Service-Client konfiguriert, wenn der DHCP-Client nach der Installation von Oracle Solaris konfiguriert wurde.

  Informationen zum Verwenden von Namen-Services mit DHCP-Clients finden Sie unter „DHCP -Clientsysteme und Namen-Services“ auf Seite 468.

DHCP-Clientsysteme mit mehreren Netzwerkschnittstellen

Der DHCP-Client kann mehrere Schnittstellen eines Systems gleichzeitig verwalten. Bei diesen Schnittstellen kann es sich um physikalische oder um logische Schnittstellen handeln. Jede Schnittstelle verfügt über eine eigene IP-Adresse und eine individuelle Leasing-Zeit. Wenn mehrere Netzwerkschnittstellen für DHCP konfiguriert sind, gibt der Client individuelle Anforderungen zur Konfiguration dieser Schnittstellen aus. Der Client pflegt für jede Schnittstelle einen individuellen Satz an Netzwerkkonfigurationsparametern. Einige Parameter gelten global, obwohl sie separat gespeichert werden. Diese globalen Parameter gelten für das gesamte System und nicht nur für eine bestimmte Netzwerkschnittstelle.

Beispiele für globale Parameter sind Hostname, NIS-Domänenname und Zeitzone. Globale Parameter weisen in der Regel für jede Schnittstelle einen anderen Wert auf. Es kann jedoch für jeden globalen Parameter, der einem System zugeordnet ist, nur ein Wert verwendet werden. Um sicherzustellen, dass es nur eine Antwort auf eine Anfrage nach einem globalen Parameter gibt, werden nur die Parameter für die primäre Netzwerkschnittstelle verwendet. Sie können das Wort `primary` in die `/etc/dhcp.`*Schnittstelle*-Datei für die Schnittstelle einfügen, die als primäre Schnittstelle behandelt werden soll. Wird das Schlüsselwort `primary` nicht verwendet, wird die erste Schnittstelle in der alphabetischen Reihenfolge als primäre Schnittstelle betrachtet.

Der DHCP-Client verwaltet die Leasing-Zeiten für logische und physikalische Schnittstellen auf die gleiche Weise, mit Ausnahme der folgenden Einschränkung für logische Schnittstellen:

- Der DHCP-Client verwaltet keinen Standard-Routen, die logischen Schnittstellen zugewiesen sind.

Der Oracle Solaris-Kernel weist Routen den physikalischen, jedoch nicht den logischen Schnittstellen zu. Nachdem die IP-Adresse einer physikalischen Schnittstelle eingerichtet wurde, müssen die erforderlichen Standard-Routen in die Routing-Tabelle eingepflegt werden. Wird daraufhin DHCP zur Konfiguration einer logischen Schnittstelle verwendet, die dieser physikalischen Schnittstelle zugeordnet ist, sind die erforderlichen Routen bereits eingerichtet. Die logische Schnittstelle verwendet die gleichen Routen.

Läuft die Leasing-Zeit einer physikalischen Schnittstelle ab, löscht der DHCP-Client die dieser Schnittstelle zugeordneten Standard-Routen. Läuft die Leasing-Zeit einer logischen Schnittstelle ab, löscht der DHCP-Client die der logischen Schnittstelle zugeordneten Standard-Routen nicht. Die zugeordnete physikalische Schnittstelle und eventuell vorhandene weitere logische Schnittstellen können die gleichen Routen weiterverwenden.

Wenn Sie die einer von DHCP verwalteten Schnittstelle zugeordneten Standard-Routen hinzufügen oder entfernen müssen, verwenden Sie ein DHCP-Client-Ereignisskript. Lesen Sie dazu „DHCP-Client Ereignisskripten“ auf Seite 473.

Hostnamen für DHCPv4-Clients

Standardmäßig gibt der Oracle Solaris DHCPv4-Client seinen eigenen Hostnamen nicht an, da er erwartet, dass der DHCP-Server den Hostnamen bereitstellt. Der Oracle Solaris DHCPv4-Server ist standardmäßig zur Bereitstellung von Hostnamen für DHCPv4-Clients konfiguriert. Wenn Sie den Oracle Solaris DHCPv4-Client und -Server zusammen verwenden, arbeiten diese Standardeinstellungen sehr gut. Wenn Sie jedoch den Oracle Solaris DHCPv4-Client und einen DHCP-Server eines Drittanbieters verwenden, empfängt der Client eventuell keinen Hostnamen vom Server. Empfängt der Oracle Solaris DHCP-Client keinen Hostnamen über DHCP, sucht das Clientsystem in der `/etc/nodename`-Datei nach einem Namen, den es als Hostnamen verwenden kann. Ist diese Datei leer, wird der Hostnamen auf `unknown` gesetzt.

Stellt der DHCP-Server in der DHCP `Hostname`-Option einen Namen bereit, verwendet der Client diesen Hostnamen auch dann, wenn ein anderer Wert in der Datei `/etc/nodename` gespeichert ist. Wenn der Client einen bestimmten Hostnamen verwenden soll, können Sie den Client so konfigurieren, dass er diesen Namen anfordert. Lesen Sie dazu die folgenden Anweisungen.

Hinweis – Die folgenden Anweisungen können nicht mit allen DHCP-Servern verwendet werden. In diesem Verfahren konfigurieren Sie den Client so, dass er einen bestimmten Hostnamen an den DHCP-Server sendet und diesen in der Antwort erwartet.

Jedoch muss der DHCP-Server dieser Anforderung nicht entsprechen, und einige Server entsprechen ihr auch nicht. Sie geben einfach einen anderen Namen zurück.

So konfigurieren Sie einen Oracle Solaris DHCPv4-Client zur Anforderung eines bestimmten Hostnamens

1. **Melden Sie sich als Superuser bei einem Clientsystem an und nehmen Sie die folgenden Änderungen an der `/etc/default/dhcpagent`-Datei vor.**

2. **Suchen Sie das Schlüsselwort `REQUEST_HOSTNAME` in der Datei `/etc/default/dhcpagent` und ändern Sie es wie folgt:**

   ```
   REQUEST_HOSTNAME=yes
   ```

   Falls sich ein Kommentarzeichen (#) vor `REQUEST_HOSTNAME` befindet, löschen Sie es. Sollte das Schlüsselwort `REQUEST_HOSTNAME` nicht vorhanden sein, fügen Sie es ein.

3. **Fügen Sie zur Datei `/etc/hostname.`*Schnittstelle* auf dem Client-System die folgende Zeile hinzu:**

   `inet` *Hostname*

   Hostname ist der Name, den der Client verwenden soll.

4. **Geben Sie die folgenden Befehle ein, damit der Client nach dem erneuten Booten eine vollständige DHCP-Aushandlung durchführt:**

   ```
   # ifconfig interface dhcp release
   # reboot
   ```

   Die auf dem Client zwischengespeicherten DHCP-Daten werden gelöscht. Der Client startet das Protokoll zur Anforderung neuer Konfigurationsinformationen neu. Hierzu gehört auch ein neuer Hostname. Zunächst stellt der DHCP-Server sicher, dass der Hostname noch von keinem anderen System im Netzwerk verwendet wird. Dann weist er dem Client den Hostnamen zu. Der DHCP-Server kann die Namen-Services mit dem Hostnamen des Clients aktualisieren, wenn er dazu konfiguriert wurde.

   Soll der Hostname zu einem späteren Zeitpunkt geändert werden, wiederholen Sie Schritt 3 und Schritt 4.

DHCP -Clientsysteme und Namen-Services

Oracle Solaris-Systeme unterstützen die folgenden Namen-Services: DNS, NIS, NIS+ und einen lokalen Datenspeicher (`/etc/inet/hosts`). Jeder Namen-Service erfordert bestimmte Konfigurationsschritte. Die Switch-Konfigurationsdatei des Namen-Service (siehe `nsswitch.conf(4)`) muss entsprechend des zu verwendenden Namen-Services eingerichtet werden.

Bevor ein DHCP-Clientsystem einen Namen-Service verwenden kann, müssen Sie das System als einen Client des Namen-Service konfigurieren. In der Standardeinstellung, und sofern nicht anderweitig während der Systeminstallation konfiguriert, werden nur lokale Dateien verwendet.

In der folgenden Tabelle sind die Punkte zusammengefasst, die bei den verschiedenen Namen-Services und DHCP beachtet werden müssen. Die Tabelle enthält Links zu der Dokumentation, die Sie beim Einrichten von Clients für den jeweiligen Namen-Service unterstützt.

TABELLE 16–1 Client-Setup-Informationen zum Namen-Service für DHCP-Clientsysteme

Namen-Service	Client-Setup-Informationen

NIS	Wenn Sie Oracle Solaris DHCP verwenden, um Informationen zu einer Oracle Solaris-Netzwerkinstallation zu senden, können Sie ein Konfigurationsmakro erstellen, in dem die Optionen `NISservs` und `NISdmain` enthalten sind. Diese Optionen übergeben die IP-Adressen der NIS-Server und den NIS-Domänennamen an den Client. Der Client wird dann automatisch ein NIS-Client.
	
	Wenn ein DHCP-Clientsystem Oracle Solaris ausführt, wird der NIS-Clients nicht automatisch auf dem System konfiguriert, wenn der DHCP-Server NIS-Informationen an den Client sendet.
	
	Wurde der DHCP-Server so konfiguriert, dass er NIS-Informationen an das DHCP-Clientsystem sendet, können Sie die an den Client übergebenen Werte anzeigen. Dazu geben Sie den Befehl `dhcpinfo` wie folgt auf dem Client ein:
	
	`# /sbin/dhcpinfo NISdmain`
	
	`# /sbin/dhcpinfo NISservs`
	
	Hinweis – Bei DHCPv6 beziehen Sie `-v6` und andere Protokollschlüsselwörter in den Befehl ein.
	
	`# /sbin/dhcpinfo -v6 NISDomain`
	
	`# /sbin/dhcpinfo -v6 NISServers`
	
	Die für den NIS-Domänennamen und NIS-Server zurückgegebenen Werte verwenden Sie zum Einrichten des Systems als NIS-Client.
	
	Sie richten einen NIS-Client standardmäßig für ein Oracle Solaris DHCP-Clientsystem ein. Dies wird in Kapitel 5, „Setting Up and Configuring NIS Service" in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* beschrieben.
	
	Tipp – Sie können ein Skript schreiben, das `dhcpinfo` und `ypinit` verwendet, um die Konfiguration des NIS-Client auf DHCP-Clientsystemen zu automatisieren.

TABELLE 16–1 Client-Setup-Informationen zum Namen-Service für DHCP-Clientsysteme *(Fortsetzung)*

Namen-Service	Client-Setup-Informationen
NIS+	Wenn der NIS+-Client für ein DHCP-Clientsystem auf konventionelle Weise eingerichtet wird, könnte der DHCP-Server gelegentlich unterschiedliche Adressen an den Client ausgeben. Dies führt zu Sicherheitsproblemen, da die NIS+-Sicherheit die IP-Adresse als Teil der Konfiguration einschließt. Um sicherzustellen, dass Ihr Client jedes Mal die gleiche Adresse erhält, richten Sie den NIS+-Client für ein DHCP-Clientsystem nicht-standardmäßig ein. Dies wird unter „Einrichten von DHCP-Clients als NIS+-Clients" auf Seite 470 beschrieben. Falls dem DHCP-Clientsystem manuell eine IP-Adresse zugewiesen wurde, so ist die Client-Adresse immer gleich. In diesem Fall richten Sie den NIS+-Client standardmäßig ein. Dies wird unter „Setting Up NIS+ Client Machines" in *System Administration Guide: Naming and Directory Services (NIS+)* beschrieben.
`/etc/inet/hosts`	Sie müssen die Datei `/etc/inet/hosts` für ein DHCP-Clientsystem einrichten, das `/etc/inet/hosts` als Namen-Service verwendet. Der Hostname des DHCP-Clientsystems wird mithilfe der DHCP-Tools der eigenen `/etc/inet/hosts`-Datei hinzugefügt. Den `/etc/inet/hosts`-Dateien anderer Systeme im Netzwerk müssen Sie den Hostnamen jedoch manuell hinzufügen. Wenn das DHCP-Serversystem `/etc/inet/hosts` zur Namensauflösung verwendet, müssen Sie darüber hinaus den Hostnamen des Clients auf dem Server manuell hinzufügen.
DNS	Wenn das DHCP-Clientsystem den DNS-Domänennamen über DHCP bezieht, wird die `/etc/resolv.conf`-Datei auf dem Clientsystem automatisch konfiguriert. Darüber hinaus wird die Datei `/etc/nsswitch.conf` automatisch aktualisiert, und `dns` wird hinter den anderen Namen-Services in der Suchreihenfolge an die Zeile `hosts` angefügt. Weitere Informationen zu DNS finden Sie im *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* .

Einrichten von DHCP-Clients als NIS+-Clients

Sie können den NIS+-Namen-Service auf Oracle Solaris-Systemen einsetzen, die als DHCP-Clients konfiguriert sind. Stellt Ihr DHCP-Server jedoch zu verschiedenen Zeiten unterschiedliche Adressen bereit, umgeht dies teilweise eine der Funktionen von NIS+. die die Sicherheit verbessern sollen: die Erstellung von Data Encryption Standard (DES)-Berechtigungsnachweisen. Aus Sicherheitsgründen müssen Sie den DHCP-Server so konfigurieren, dass er jederzeit die gleiche Adresse bereitstellt. Wenn Sie einen NIS+-Client so konfigurieren, dass er *kein* DHCP verwendet, können Sie einmalige DES-Berechtigungsnachweise für den Client beim NIS+-Server hinzufügen. Es gibt verschiedene Möglichkeiten, Berechtigungsnachweise zu erstellen. Hierzu zählen das Verwenden des `nisclient`-Skripts oder der `nisaddcred`-Befehl.

Zum Erzeugen von NIS+-Berechtigungsnachweisen muss der Client über einen statischen Hostnamen verfügen, so dass die Berechtigungsnachweise erstellt und gespeichert werden

können. Wenn Sie NIS+ und DHCP verwenden möchten, müssen Sie identische Berechtigungsnachweise erstellen, die für alle Hostnamen von DHCP-Clients verwendet werden. Auf diese Weise kann der Client die gleichen DES-Berechtigungsnachweise verwenden, ungeachtet dessen, welche IP-Adresse mit zugehörigem Hostnamen ein DHCP-Client erhält.

Das folgende Verfahren zeigt, wie Sie identische Berechtigungsnachweise für alle DHCP-Hostnamen erstellen. Dieses Verfahren ist nur dann gültig, wenn Sie die von den DHCP-Clients verwendeten Hostnamen kennen. Angenommen, der DHCP-Server erzeugt die Hostnamen, so kennen Sie die möglichen Hostnamen, die ein Client erhalten kann.

▼ So richten Sie Oracle Solaris DHCP-Clients als NIS+-Clients ein

Ein DHCP-Clientsystem, das als NIS+-Client konfiguriert werden soll, muss Berechtigungsnachweise verwenden, die einem anderen NIS+-Clientsystem in der NIS+-Domäne gehören. Dieses Verfahren erzeugt lediglich Berechtigungsnachweise für das System, die nur für den Superuser gelten, der beim System angemeldet ist. Andere Benutzer, die sich beim DHCP-Clientsystem anmelden, müssen über eigene einmalige Berechtigungsnachweise auf dem NIS+-Server verfügen. Diese Berechtigungsnachweise werden entsprechend dem Verfahren im *System Administration Guide: Naming and Directory Services (NIS+)* erzeugt.

1. **Erstellen Sie die Berechtigungsnachweise für einen Client, indem Sie den folgenden Befehl auf einem NIS+-Server eingeben:**

   ```
   # nisgrep nisplus-client-name cred.org_dir > /tmp/file
   ```

   Dieser Befehl schreibt den Tabelleneintrag `cred.org_dir` für den NIS+-Client in eine temporäre Datei.

2. **Zum Anzeigen des Inhalts der temporären Datei geben Sie den Befehl `cat` ein.**

   Oder verwenden Sie einen Texteditor.

3. **Kopieren Sie die zu verwendenden Berechtigungsnachweise für DHCP-Clients.**

   Sie müssen den PublicKey und den PrivateKey kopieren. Dies sind lange Strings mit Zahlen und Buchstaben, die durch Doppelpunkte voneinander getrennt sind. Die Berechtigungsnachweise müssen in den Befehl eingefügt werden, der im nächsten Schritt ausgegeben wird.

4. **Fügen Sie die Berechtigungsnachweise für einen DHCP-Client hinzu, indem Sie den folgenden Befehl eingeben:**

   ```
   # nistbladm -a cname=" dhcp-client-name@nisplus-domain" auth_type=DES \
   auth_name="unix.dhcp-client-name@nisplus-domain" \
   public_data=copied-public-key \
   private_data=copied-private-key
   ```

Für *kopierter-PublicKey* fügen Sie die Informationen des PublicKey ein, die Sie aus der temporären Datei kopiert haben. Für *kopierter-PrivateKey* fügen Sie die Informationen des PrivateKey ein, die Sie aus der temporären Datei kopiert haben.

5. **Kopieren Sie Dateien standortfern vom NIS+-Clientsystem zum DHCP-Clientsystem, indem Sie die folgenden Befehle auf einem DHCP-Clientsystem eingeben:**

```
# rcp nisplus-client-name:/var/nis/NIS_COLD_START /var/nis
# rcp nisplus-client-name:/etc/.rootkey /etc
# rcp nisplus-client-name:/etc/defaultdomain /etc
```

Falls Sie die Meldung „Zugriff verweigert" angezeigt wird, gestattet das System eventuell kein remotes Kopieren. In diesem Fall können Sie die Dateien als normaler Benutzer an einen Zwischenspeicherort kopieren. Kopieren Sie die Dateien dann als Superuser vom Zwischenspeicherort an den korrekten Speicherort auf dem DHCP-Clientsystem.

6. **Kopieren Sie die richtige Switch-Datei des Namen-Service für NIS+, indem Sie den folgenden Befehl auf einem DHCP-Clientsystem ausführen:**

```
# cp /etc/nsswitch.nisplus /etc/nsswitch.conf
```

7. **Booten Sie das DHCP-Clientsystem neu.**

Das DHCP-Clientsystem sollte jetzt in der Lage sein, NIS+-Services zu verwenden.

Beispiel 16–1 Einrichten eines Oracle Solaris DHCP-Clientsystems als NIS+-Client

Im folgenden Beispiel wird ein System `nisei` angenommen, bei dem es sich um einen NIS+-Client in der NIS+-Domäne `dev.example.net` handelt. Darüber hinaus gibt es ein DHCP-Clientsystem, `dhow`, und Sie möchten `dhow` als NIS+-Client konfigurieren.

```
    (First log in as superuser on the NIS+ server)
# nisgrep nisei cred.org_dir > /tmp/nisei-cred
# cat /tmp/nisei-cred
nisei.dev.example.net.:DES:unix.nisei@dev.example.net:46199279911a84045b8e0
c76822179138173a20edbd8eab4:90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830
c05bc1c724b
# nistbladm -a cname="dhow@dev.example.net." \
auth_type=DES auth_name="unix.dhow@dev.example.net" \
public_data=46199279911a84045b8e0c76822179138173a20edbd8eab4 \
private_data=90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830\
c05bc1c724b
# rlogin dhow
    (Log in as superuser on dhow)
# rcp nisei:/var/nis/NIS_COLD_START /var/nis
# rcp nisei:/etc/.rootkey /etc
# rcp nisei:/etc/defaultdomain /etc
# cp /etc/nsswitch.nisplus /etc/nsswitch.conf
# reboot
```

Das DHCP-Clientsystem dhow sollte jetzt in der Lage sein, NIS+-Services zu verwenden.

Beispiel 16–2 Hinzufügen von Berechtigungsnachweisen mit einem Skript

Wenn Sie zahlreiche DHCP-Clientsysteme als NIS+-Clients einrichten möchten, können Sie ein Skript schreiben. Mit einem Skript können Sie schnell Einträge zur NIS+-Tabelle cred.org_dir hinzufügen. Im Folgenden ist ein Beispielskript aufgeführt.

```
#! /usr/bin/ksh
#
# Copyright (c) by Sun Microsystems, Inc. All rights reserved.
#
# Sample script for cloning a credential. Hosts file is already populated
# with entries of the form dhcp-[0-9][0-9][0-9]. The entry we're cloning
# is dhcp-001.
#
#
PUBLIC_DATA=6e72878d8dc095a8b5aea951733d6ea91b4ec59e136bd3b3
PRIVATE_DATA=3a86729b685e2b2320cd7e26d4f1519ee070a60620a93e48a8682c5031058df4
HOST="dhcp-"
DOMAIN="mydomain.example.com"

for
i in 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019
do
     print - ${HOST}${i}
     #nistbladm -r [cname="${HOST}${i}.${DOMAIN}."]cred.org_dir
     nistbladm -a cname="${HOST}${i}.${DOMAIN}." \
         auth_type=DES auth_name="unix.${HOST}${i}@${DOMAIN}" \
         public_data=${PUBLIC_DATA} private_data=${PRIVATE_DTA} cred.org_Dir
done

exit 0
```

DHCP-Client Ereignisskripten

Sie können den Oracle Solaris DHCP-Client so konfigurieren, dass er ein ausführbares Programm oder ein Skript aufruft, das eine für das Clientsystem geeignete Aktion ausführt. Dieses Programm oder Skript, das als *Ereignisskript* bezeichnet wird, wird automatisch ausgeführt, nachdem bestimmte DHCP-Leasing-Ereignisse aufgetreten sind. Das Ereignisskript kann zum Ausführen anderer Befehle, Programme oder Skripten als Reaktion auf bestimmte Leasing-Ereignisse verwendet werden. Zum Verwenden dieser Funktion müssen Sie eigene Ereignisskripten bereitstellen.

Die folgenden Ereignis-Schlüsselwörter werden von dhcpagent-Daemon verwendet, um DHCP-Leasing-Ereignisse zu kennzeichnen:

Ereignis-Schlüsselwort	Beschreibung
BOUND und BOUND6	Die Schnittstelle wird für DHCP konfiguriert. Der Client erhält eine Bestätigungsnachricht (DHCPv4 ACK) oder (DHCPv6 Reply)

vom DHCP-Server, die eine Leasing-Anforderung nach einer IP-Adresse gewährt. Das Ereignisskript wird unmittelbar nach der erfolgreichen Konfiguration der Schnittstelle aufgerufen.

`EXTEND` und `EXTEND6` — Der Client verlängert erfolgreich ein Leasing. Das Ereignisskript wird aufgerufen, unmittelbar nachdem der Client die Bestätigungsnachricht vom DHCP-Server über die Erneuerungsanforderung erhalten hat.

`EXPIRE` und `EXPIRE6` — Das Leasing läuft ab, wenn die Leasing-Zeit gestrichen ist. Bei DHCPv4 wird das Ereignisskript aufgerufen, unmittelbar bevor die geleaste Adresse von der Schnittstelle entfernt und die Schnittstelle als offline gekennzeichnet wird. Bei DHCPv6 wird das Ereignisskript aufgerufen, unmittelbar bevor die letzte verbleibende geleaste Adresse von der Schnittstelle entfernt wird.

`DROP` und `DROP6` — Der Client verwirft das Leasing, um die Schnittstelle aus der DHCP-Verwaltung zu entfernen. Das Ereignisskript wird aufgerufen, unmittelbar bevor die Schnittstelle aus der DHCP-Verwaltung entfernt wird.

`RELEASE` und `RELEASE6` — Der Client gibt die IP-Adresse frei. Das Ereignisskript wird ausgeführt, unmittelbar bevor der Client die Adresse der Schnittstelle freigibt und `RELEASE`- oder DHCPv6 `Release`-Pakete an den DHCP-Server sendet.

`INFORM` und `INFORM6` — Eine Schnittstelle bezieht über die DHCPv4 `INFORM`- oder die DHCPv6 `Information-Request`-Nachricht neue oder aktualisierte Konfigurationsinformationen von einem DHCP-Server. Dieser Ereignisse treten auf, wenn der DHCP-Client nur Konfigurationsinformationen vom Server und kein Leasing für eine IP-Adresse bezieht.

`LOSS6` — Während des Ablaufs der Leasing-Zeit, wenn noch mindestens ein Leasing gültig ist, wird das Ereignisskript aufgerufen, bevor abgelaufene Adressen entfernt werden. Die entfernten Adressen werden mit dem Flag `IFF_DEPRECATED` gekennzeichnet.

Bei jedem dieser Ereignisse ruft der `dhcpagent`-Daemon den folgenden Befehl auf:

`/etc/dhcp/eventhook` *interface event*

dabei steht *Schnittstelle* für die Schnittstelle, die DHCP verwendet und *Ereignis* ist eines der oben beschriebenen Ereignisschlüsselwörter. Angenommen, die Schnittstelle `ce0` wurde als erstes für DHCP konfiguriert, so ruft der `dhcpagent`-Daemon das Ereignisskript wie folgt auf:

```
/etc/dhcp/eventhook ce0 BOUND
```

Um ein Ereignisskript verwenden zu können, müssen Sie Folgendes ausführen:

- Benennen der ausführbaren Datei /etc/dhcp/eventhook.
- Einstellen des Eigners der Datei auf root.
- Einstellen der Berichtigungen auf 755 (rwxr-xr-x).
- Schreiben Sie das Skript oder Programm, um eine Abfolge von Aktionen als Reaktion auf eines der dokumentierten Ereignisse auszuführen. Da Sun eventuell neue Ereignismodelle hinzufügt, muss das Programm alle nicht erkannten Ereignisse oder solche, die keine Aktionen erfordern, stillschweigend ignorieren. Beispielsweise könnte das Programm oder Skript in eine Protokolldatei schreiben, wenn das Ereignis RELEASE lautet und alle anderen Ereignisse ignorieren.
- Sorgen Sie dafür, das Skript bzw. Programm nicht-interaktiv ist. Bevor das Ereignis wird aufgerufen wird, sind stdin, stdout und stderr mit /dev/null verbunden. Um die Ausgabe oder Fehler zu sehen, müssen Sie zu einer Datei umleiten.

Das Ereignisskript übernimmt die Programmumgebung vom dhcpagent-Daemon und wird mit root-Berechtigungen ausgeführt. Das Skript kann das Dienstprogramm dhcpinfo verwenden, um ggf. weitere Informationen zur Schnittstelle zu beziehen. Weitere Informationen finden Sie in der Manpage dhcpinfo(1).

Der dhcpagent-Daemon wartet, bis das Ereignisskript für alle Ereignisse beendet ist. Wenn das Ereignisskript nach 55 Sekunden nicht beendet ist, sendet der dhcpagent-Daemon ein SIGTERM-Signal an den Skriptprozess. Wird der Prozess nach weiteren 3 Sekunden nicht beendet, sendet der Daemon ein SIGKILL-Signal, um den Prozess zu beenden.

Ein Beispiel eines Ereignisskripts finden Sie in der Manpage dhcpagent(1M).

Beispiel 16–3 zeigt, wie Sie ein DHCP-Ereignisskript verwenden, um den Inhalt der /etc/resolv.conf-Datei auf dem neuesten Stand zu halten. Wenn die Ereignisse BOUND und EXTEND auftreten, ersetzt das Skript die Namen von Domänenserver und Namensserver. Wenn die Ereignisse EXPIRE, DROP und RELEASE auftreten, entfernt das Skript die Namen von Domänenserver und Namensserver aus der Datei.

Hinweis – Das Beispielskript geht davon aus, dass DHCP die autoritative Quelle für die Namen von Domänenserver und Namensserver ist. Weiterhin geht das Skript davon aus, dass alle Schnittstellen unter der Verwaltung von DHCP konsistente und aktuelle Informationen zurückgeben. Diese Annahmen spiegeln eventuell nicht die Bedingungen auf Ihrem System wider.

BEISPIEL 16–3 Ereignisskript zur Aktualisierung der Datei /etc/resolv.conf

```
#!/bin/ksh -p

PATH=/bin:/sbin export PATH
```

BEISPIEL 16–3 Ereignisskript zur Aktualisierung der Datei `/etc/resolv.conf` *(Fortsetzung)*

```
umask 0222

# Refresh the domain and name servers on /etc/resolv.conf

insert ()
{
    dnsservers=‘dhcpinfo -i $1 DNSserv‘
    if [ -n "$dnsservers" ]; then
        # remove the old domain and name servers
        if [ -f /etc/resolv.conf ]; then
            rm -f /tmp/resolv.conf.$$
            sed -e ’/^domain/d’ -e ’/^nameserver/d’ \
                /etc/resolv.conf > /tmp/resolv.conf.$$
        fi

        # add the new domain
        dnsdomain=‘dhcpinfo -i $1 DNSdmain‘
        if [ -n "$dnsdomain" ]; then
            echo "domain $dnsdomain" >> /tmp/resolv.conf.$$
        fi

        # add new name servers
        for name in $dnsservers; do
            echo nameserver $name >> /tmp/resolv.conf.$$
        done
        mv -f /tmp/resolv.conf.$$ /etc/resolv.conf
    fi
}

# Remove the domain and name servers from /etc/resolv.conf

remove ()
{
    if [ -f /etc/resolv.conf ]; then
        rm -f /tmp/resolv.conf.$$
        sed -e ’/^domain/d’ -e ’/^nameserver/d’ \
            /etc/resolv.conf > /tmp/resolv.conf.$$
        mv -f /tmp/resolv.conf.$$ /etc/resolv.conf
    fi
}

case $2 in
BOUND | EXTEND)
    insert $1
    exit 0
    ;;
EXPIRE | DROP | RELEASE)
    remove
    exit 0
    ;;
*)
    exit 0
    ;;
esac
```

KAPITEL 17

DHCP-Fehlerbehebung (Referenz)

Dieses Kapitel enthält Informationen, die Ihnen dabei helfen, Probleme bei der Konfiguration eines DHCP-Servers oder -Clients zu beheben. Außerdem hilft Ihnen dieses Kapitel bei Problemen, die sich eventuell nach der Konfiguration bei der Verwendung von DHCP einstellen.

Dieses Kapitel enthält die folgenden Informationen:

- „Beheben von Problemen mit dem DHCP-Server" auf Seite 477
- „Troubleshooting DHCP Client Configuration Problems" auf Seite 484

Informationen zur Konfiguration Ihres DHCP-Servers finden Sie in Kapitel 14, „Konfiguration des DHCP-Services (Aufgaben)". Informationen zur Konfiguration Ihres DHCP-Clients finden Sie in „Aktivieren und Deaktivieren eines Oracle Solaris DHCP-Clients" auf Seite 462.

Beheben von Problemen mit dem DHCP-Server

Die Probleme, die bei der Konfiguration des Servers auftreten können, fallen in zwei Kategorien:

- „NIS+-Probleme und der DHCP-Datenspeicher" auf Seite 477
- „Fehler bei der IP-Adresszuweisung unter DHCP" auf Seite 481

NIS+-Probleme und der DHCP-Datenspeicher

Wenn Sie NIS+ als DHCP-Datenspeicher verwenden, lassen sich die eventuell auftretenden Probleme wie folgt kategorisieren:

- „NIS+ kann nicht als DHCP-Datenspeicher gewählt werden" auf Seite 478
- „NIS+ ist nicht korrekt für den DHCP-Datenspeicher konfiguriert" auf Seite 478
- „NIS+-Zugriffsprobleme auf den DHCP-Datenspeicher" auf Seite 479

NIS+ kann nicht als DHCP-Datenspeicher gewählt werden

Wenn Sie versuchen, NIS+ als Datenspeicher zu verwenden, bietet DHCP Manager NIS+ nicht als Auswahlmöglichkeit für den Datenspeicher an. Verwenden Sie den Befehl `dhcpconfig`, wird eventuell eine Meldung angezeigt, die darauf hinweist, dass NIS+ anscheinend nicht installiert ist und somit nicht ausgeführt werden kann. Beide Symptome deuten daraufhin, dass NIS+ für diesen Server nicht konfiguriert wurde, obwohl NIS+ offenbar in diesem Netzwerk verwendet wird. Bevor Sie NIS+ als einen Datenspeicher auswählen können, muss das Serversystem als ein NIS+-Client konfiguriert werden.

Um das DHCP-Serversystem als NIS+-Client einrichten können, müssen die folgenden Bedingungen zutreffen:

- Die Domäne muss bereits konfiguriert sein.
- Der Master-Server der NIS+-Domäne muss ausgeführt werden.
- Die Tabellen des Master-Servers müssen ausgefüllt sein.
- Die hosts-Tabelle muss einen Eintrag für das neue Clientsystem, das DHCP-Serversystem, enthalten.

„Setting Up NIS+ Client Machines“ in *System Administration Guide: Naming and Directory Services (NIS+)* enthält ausführliche Informationen zur Konfiguration eines NIS+-Clients.

NIS+ ist nicht korrekt für den DHCP-Datenspeicher konfiguriert

Wenn Sie NIS+ erfolgreich mit DHCP verwenden können, treten eventuell Fehler auf, wenn Sie Änderungen an NIS+ vornehmen. Die Änderungen könnten Konfigurationsprobleme verursachen. Suchen Sie in den folgenden Problembeschreibungen und Lösungen nach einer möglichen Ursache Ihrer Konfigurationsprobleme.

Problem: Root-Objekt existiert nicht in der NIS+-Domäne.

Lösung: Geben Sie folgenden Befehl ein:

```
/usr/lib/nis/nisstat
```

Dieser Befehl zeigt die Statistiken der Domäne an. Wenn das Root-Objekt nicht existiert, werden keine Statistiken zurückgegeben.

Richten Sie die NIS+-Domäne entsprechend den Angaben im *System Administration Guide: Naming and Directory Services (NIS+)* ein.

Problem: NIS+ wird nicht für die `passwd`- und `publickey` -Informationen verwendet.

Lösung: Geben Sie den folgenden Befehl ein, um die Konfigurationsdatei für den Namen-Service-Switch anzuzeigen:

```
cat /etc/nsswitch.conf
```

Prüfen Sie die Einträge `passwd` und `publickey` auf das Schlüsselwort „nisplus“. Informationen zur Konfiguration des Namen-Service-Switch finden Sie im *System Administration Guide: Naming and Directory Services (NIS+)* .

Problem: Der Domänenname ist leer.

Lösung: Geben Sie folgenden Befehl ein:

```
domainname
```

Wenn der Befehl einen leeren String zurückgibt, wurde kein Domänenname für die Domäne eingerichtet. Verwenden Sie lokale Dateien als Datenspeicher oder richten Sie eine NIS+-Domäne für Ihr Netzwerk ein. Informationen dazu finden Sie im *System Administration Guide: Naming and Directory Services (NIS+)* .

Problem: Die Datei `NIS_COLD_START` ist nicht vorhanden.

Lösung: Geben Sie den folgenden Befehl auf dem Serversystem ein, um festzustellen, ob die Datei vorhanden ist:

```
cat /var/nis/NIS_COLD_START
```

Verwenden Sie lokale Dateien als Ihren Datenspeicher oder erstellen Sie einen NIS+-Client. Informationen dazu finden Sie im *System Administration Guide: Naming and Directory Services (NIS+)* .

NIS+-Zugriffsprobleme auf den DHCP-Datenspeicher

NIS+-Zugriffsprobleme verursachen eventuell Fehlermeldungen über falsche DES-Berechtigungsnachweise oder nicht ausreichende Berechtigungen zum Aktualisieren von NIS+-Objekten oder -Tabellen. Suchen Sie in den folgenden Problembeschreibungen und Lösungen nach möglichen Ursachen für die bei Ihnen aufgetretenen NIS+-Zugriffsfehler.

Problem: Das DHCP-Serversystem hat kein Recht zum Erstellen des `org_dir`-Objekts in der NIS+-Domäne.

Lösung: Geben Sie folgenden Befehl ein:

```
nisls -ld org_dir
```

Die Zugriffsrechte sind im Format `r---rmcdrmcdr---` aufgeführt. Dabei gelten die Berechtigungen jeweils für die Klassen „Niemand“, „Eigentümer“, „Gruppe“ und „Global“. Der Eigentümer des Objekts ist als Nächstes aufgeführt.

Normalerweise bietet das Verzeichnisobjekt `org_dir` den Klassen „Eigentümer“ und „Gruppe“ vollständige Rechte. Die vollständigen Rechte umfassen „Lesen“, „Ändern“, „Erstellen“ und „Vernichten“. Das Verzeichnisobjekt `org_dir` bietet den Klassen „Global“ und „Niemand“ nur Lesezugriff.

Der DHCP-Servername muss entweder als Eigentümer des `org_dir`-Objekts oder als Hauptelement in der Gruppe aufgeführt sein. Die Gruppe muss über das Recht zum Erstellen verfügen. Listen Sie die Gruppe mit dem folgenden Befehl auf:

```
nisls -ldg org_dir
```

Mit dem Befehl `nischmod` können Sie ggf. die Berechtigungen für das `org_dir`-Objekt ändern. Um beispielsweise das Recht zum Erstellen für die Gruppe hinzuzufügen, geben Sie den folgenden Befehl ein:

```
nischmod g+c org_dir
```

Weitere Informationen finden Sie in der Manpage `nischmod(1)`.

Problem: Der DHCP-Server hat kein Recht zum Erstellen einer Tabelle unter dem `org_dir`-Objekt.

In der Regel deutet dieses Problem darauf hin, dass der Hauptname des Serversystems kein Mitglied der Eigner-Gruppe des `org_dir`-Objekts ist, oder dass keine Eigner-Gruppe existiert.

Lösung: Geben Sie den folgenden Befehl ein, um den Eigner-Gruppennamen zu finden:

```
niscat -o org_dir
```

Suchen Sie nach einer Zeile ähnlich der Folgenden:

`Group : "admin.example.com."`

Listen Sie die Hauptnamen in der Gruppe mit dem folgenden Befehl auf:

```
nisgrpadm -l groupname
```

Mit dem folgenden Befehl werden beispielsweise die Hauptnamen der Gruppe `admin.example.com` aufgeführt:

`nisgrpadm -l admin.example.com`

Der Name des Serversystems sollte als explizites Mitglied der Gruppe aufgeführt oder als implizites Mitglied der Gruppe enthalten sein. Fügen Sie ggf. den Namen des Serversystems zu der Gruppe hinzu, die den Befehl `nisgrpadm` verwendet.

Um beispielsweise den Servernamen `pacific` zur Gruppe `admin.example.com` hinzuzufügen, geben Sie den folgenden Befehl ein:

```
nisgrpadm -a admin.example.com pacific.example.com
```

Weitere Informationen finden Sie in der Manpage `nisgrpadm(1)`.

Problem: Der DHCP-Server verfügt keine gültigen Data Encryption Standard (DES)-Berechtigungsnachweise in der NIS+-Tabelle `cred`.

Lösung: Falls ein Problem mit den Berechtigungsnachweisen vorliegt, zeigt eine Fehlermeldung an, dass der Benutzer nicht über den nötigen DES-Berechtigungsnachweise im NIS+-Namen-Service verfügt.

Mit dem Befehl `nisaddcred` können Sie Sicherheitsberechtigungen für das DHCP-Serversystem hinzufügen.

Im folgenden Beispiel wird gezeigt, wie Sie DES-Berechtigungsnachweise für das System `mercury` in der Domäne `example.com` hinzufügen:

```
nisaddcred -p unix.mercury@example.com \
-P mercury.example.com. DES example.com.
```

Der Befehl fordert zur Eingabe des root-Passwort auf, dass zum Erzeugen eines verschlüsselten Sicherheitsschlüssels erforderlich ist.

Weitere Informationen finden Sie in der Manpage `nisaddcred`(1M).

Fehler bei der IP-Adresszuweisung unter DHCP

Wenn ein Client versucht, eine IP-Adresse zu beziehen oder zu überprüfen, werden eventuell Fehlermeldungen im `syslog` oder in der Ausgabe im Server-Debugging-Modus protokolliert. Die folgende Liste der häufigsten Fehlermeldungen gibt mögliche Ursachen und Lösungen an.

`Es ist keine` *n.n.n.n* `dhcp-Netzwerktabelle für das Netzwerk des DHCP-Client vorhanden`

Grund: Ein Client fordert eine bestimmte IP-Adresse an oder versucht, die Leasing-Zeit für die aktuelle IP-Adresse zu verlängern. Der DHCP-Server kann die DHCP-Netzwerktabelle für diese Adresse nicht finden.

Lösung: Die DHCP-Netzwerktabelle wurde eventuell versehentlich gelöscht. Sie können die Netzwerktabelle neu erstellen, indem Sie das Netzwerk erneut mit DHCP Manager oder den Befehl `dhcpconfig` hinzufügen.

`ICMP ECHO-Antwort an OFFER-Kandidat:` *n.n.n.n*`, deaktivieren.`

Grund: Die IP-Adresse, die einem DHCP-Client angeboten werden soll, wird bereits verwendet. Dieses Problem kann auftreten, wenn mehrere DHCP-Server Eigentümer der Adresse sind. Außerdem könnte dieses Problem auftreten, wenn eine Adresse manuell für einen nicht-DHCP-Netzwerkclient konfiguriert wurde.

Lösung: Stellen Sie fest, wer der wahre Eigentümer der Adresse ist. Berichtigen Sie entweder die DHCP-Serverdatenbank oder die Netzwerkkonfiguration des Hosts.

`ICMP ECHO-Antwort an OFFER-Kandidat:` *n.n.n.n*`. Kein entsprechender DHCP-Netzwerkdatensatz.`

Grund: Die IP-Adresse, die einem DHCP-Client angeboten werden soll, verfügt nicht über einen Datensatz in einer Netzwerktabelle. Dieser Fehler deutet darauf hin, dass der Datensatz der IP-Adresse aus der DHCP-Netzwerktabelle gelöscht wurde, nachdem die Adresse ausgewählt wurde. Dieser Fehler kann nur in der kurzen Zeit auftreten, bevor die Prüfung auf eine doppelt vorhandene Adresse abgeschlossen ist.

Lösung: Zeigen Sie den Inhalt der DHCP-Netzwerktabelle mit DHCP Manager oder dem Befehl `pntadm` an. Falls die IP-Adresse fehlt, erstellen Sie sie mit DHCP Manager, indem Sie den Befehl „Erzeugen" im Menü „Bearbeiten" auf die Registerkarte „Adressen" auswählen. Sie können die IP-Adresse auch mit dem Befehl `pntadm` erzeugen.

`DHCP-Netzwerkdatensatz für` *n.n.n.n* `ist nicht verfügbar. Anforderung wird ignoriert.`

Grund: Der Datensatz für die angeforderte IP-Adresse befindet sich nicht in der DHCP-Netzwerktabelle. Die Anforderung wird vom Server ignoriert.

Lösung: Zeigen Sie den Inhalt der DHCP-Netzwerktabelle mit DHCP Manager oder dem Befehl `pntadm` an. Falls die IP-Adresse fehlt, erstellen Sie sie mit DHCP Manager, indem Sie den Befehl „Erzeugen" im Menü „Bearbeiten" auf die Registerkarte „Adressen" auswählen. Sie können die Adresse auch mit dem Befehl `pntadm` erzeugen.

n.n.n.n `ist derzeit als nicht verwendbar gekennzeichnet.`

Grund: Die angeforderte IP-Adresse kann nicht angeboten waren, da die Adresse in der Netzwerktabelle als nicht verwendbar gekennzeichnet ist.

Lösung: Sie können die Adresse mit DHCP Manager oder dem Befehl `pntadm` wieder verwendbar machen.

n.n.n.n `wurde manuell zugeordnet. Es wird keine dynamische Adresse zugeordnet.`

Grund: Der Client-ID wurde manuell eine Adresse zugeordnet, und diese Adresse ist als nicht verwendbar gekennzeichnet. Der Server kann diesem Client keine andere Adresse zuordnen.

Lösung: Sie können die Adresse mit DHCP Manager oder dem Befehl `pntadm` wieder verwendbar machen oder dem Client manuell eine andere Adresse zuordnen.

`Manuelle Zuordnung (`*n.n.n.n, Client-ID*`) hat` *n* `weitere Datensätze. Sie sollte jedoch 0 haben.`

Grund: Dem Client mit der angegebenen Client-ID wurden mehrere IP-Adressen manuell zugeordnet. Einem Client darf nur eine Adresse zugeordnet sein. Der Server wählt die zuletzt manuell zugeordnete Adresse in der Netzwerktabelle aus.

Lösung: Entfernen Sie die zusätzlich manuell zugeordneten Adressen mithilfe von DHCP Manager oder dem Befehl `pntadm`.

`Keine weiteren IP-Adressen in Netzwerk` *n.n.n.n*`.`

Grund: Alle IP-Adressen, die derzeit von DHCP im angegebenen Netzwerk verwaltet werden, wurden bereits zugeordnet.

Lösung: Erstellen Sie neue IP-Adressen für dieses Netzwerk mithilfe von DHCP Manager oder dem Befehl `pntadm`.

`Client:` *clientid*`-Leasing für` *n.n.n.n* `abgelaufen.`

Grund: Das Leasing war nicht aushandelbar und läuft ab.

Lösung: Der Client muss das Protokoll automatisch neu starten, um ein neues Leasing zu beziehen.

`Angebot abgelaufen für Client:` *n.n.n.n*

Grund: Der Server hat dem Client eine IP-Adresse angeboten, aber die Antwort des Clients dauerte zu lange und das Angebot ist abgelaufen.

Lösung: Der Client muss automatisch eine weitere Erkennungsmeldung ausgeben. Wenn auch für diese Meldung eine Zeitüberschreitung eintritt, erhöhen Sie den Cache-Angebot-Timeout-Wert für den DHCP-Server. Wählen Sie in DHCP Manager die Option „Ändern" im Menü „Service" aus.

`Client:` *clientid* `REQUEST (Anforderung) fehlt die angeforderte IP-Option.`

Grund: Die Client-Anforderung gibt die angeforderte IP-Adresse nicht an, daher hat der DHCP-Server die Anforderung ignoriert. Dieses Problem kann auftreten, wenn Sie einen DHCP-Client eines Drittanbieters verwenden, der nicht mit dem aktualisierten DHCP-Protokoll (RFC 2131) kompatibel ist.

Lösung: Aktualisieren Sie die Client-Software.

`Client:` *clientid* `versucht,` *n.n.n.n*`, zu erneuern, eine IP-Adresse, die nicht geleast wurde.`

Grund: Die IP-Adresse dieses Clients in der DHCP-Netzwerktabelle entspricht nicht der IP-Adresse, die der Client in seiner Erneuerungsanforderung angegeben hat. Der DHCP-Server wird das Leasing nicht erneuern. Dieses Problem kann auftreten, wenn Sie den Datensatz eines Clients löschen, obwohl der Client die IP-Adresse noch verwendet.

Lösung: Prüfen Sie die Netzwerktabelle mithilfe von DHCP Manager oder dem Befehl `pntadm`, und korrigieren Sie ggf. den Client-Datensatz. Die Client-ID sollte an die angegebene IP-Adresse gebunden sein. Ist die Client-ID nicht gebunden, ändern Sie die Eigenschaften der Adresse und fügen Sie die Client-ID hinzu.

`Client:` *clientid* `eine nicht aufgezeichnete Adresse zu bestätigen:` *n.n.n.n* `wird ignoriert.`

Grund: Der angegebene Client wurde nicht mit dieser Adresse in der DHCP-Netzwerktabelle registriert, daher wird die Anforderung von diesem DHCP-Server ignoriert.

Die Adresse wurde dem Client eventuell von einem anderen DHCP-Server im Netzwerk zugewiesen. Vielleicht haben Sie jedoch den Client-Datensatz gelöscht, obwohl der Client die IP-Adresse noch verwendet.

Lösung: Prüfen Sie die Netzwerktabelle auf diesem Server und auf anderen DHCP-Server im Netzwerk mithilfe von DHCP Manager oder dem Befehl `pntadm.` Nehmen Sie eventuell erforderliche Änderungen vor.

Sie können auch nichts unternehmen und das Leasing ablaufen lassen. Der Client fordert automatisch ein neues Adressen-Leasing an.

Wenn der Client sofort ein neues Leasing erhalten soll, starten Sie das DHCP-Protokoll auf dem Client neu, indem Sie die folgenden Befehle eingeben:

```
ifconfig interface dhcp release
ifconfig interface dhcp start
```

Troubleshooting DHCP Client Configuration Problems

Die Probleme, die bei der Konfiguration eines DHCP-Clients auftreten können, fallen in die folgenden Kategorien:

- „Kommunikationsprobleme mit dem DHCP-Server“ auf Seite 484
- „Problems With Inaccurate DHCP Configuration Information“ auf Seite 493

Kommunikationsprobleme mit dem DHCP-Server

In diesem Abschnitt werden Probleme beschrieben, die eventuell beim Hinzufügen von DHCP-Clients zum Netzwerk auftreten können.

Nachdem Sie die Client-Software aktiviert und das System neu gebootet haben, versucht der Client, den DHCP-Server zu erreichen, um seine Netzwerkkonfiguration zu beziehen. Kann der Client den Server nicht erreichen, werden eventuell Fehlermeldungen wie die Folgende angezeigt:

```
DHCP or BOOTP server not responding
```

Bevor Sie das Problem feststellen können, müssen Sie Diagnoseinformationen vom Client und Server sammeln. Dazu können Sie die folgenden Aufgaben ausführen:

1. „How to Run the DHCP Client in Debugging Mode“ auf Seite 484
2. „How to Run the DHCP Server in Debugging Mode“ auf Seite 485
3. „So verwenden Sie snoop zur Überwachung des DHCP-Netzwerkverkehrs“ auf Seite 485

Diese Aufgaben können gleichzeitig oder getrennt voneinander ausgeführt werden.

Mit den gesammelten Informationen stellen Sie fest, ob das Problem beim Client, Server oder einem Relay-Agent liegt. Anschließend können Sie nach einer Lösung suchen.

▼ How to Run the DHCP Client in Debugging Mode

Handelt es sich bei dem Client nicht um einen Oracle Solaris DHCP-Client, suchen Sie bitte in der Dokumentation Ihres Clients nach Informationen, wie der Client im Debugging-Modus ausgeführt wird.

Bei einem Oracle Solaris DHCP-Client führen Sie die folgenden Schritte aus.

1. **Melden Sie sich als Superuser beim DHCP-Clientsystem an.**

2. **Brechen Sie den DHCP-Client-Daemon ab.**

```
# pkill -x dhcpagent
```

3 Starten Sie den Daemon im Debugging-Modus neu.

```
# /sbin/dhcpagent -d1 -f &
```

Mit dem Schalter `-d` versetzen Sie den DHCP-Client in den Debugging-Modus mit der Ausführlichkeitsstufe 1. Der Schalter `-f` sorgt dafür, dass die Ausgabe an die Konsole und nicht an `syslog` gesendet wird.

4 Konfigurieren Sie die Schnittstelle so, dass sie eine DHCP-Aushandlung beginnt.

```
# ifconfig interface dhcp start
```

Ersetzen Sie *Schnittstelle* durch den Namen der Netzwerkschnittstelle des Client, z. B. `ge0`.

Wenn der Client-Daemon im Debugging-Modus ausgeführt wird, zeigt er während des Ausführens von DHCP-Anforderungen Meldungen auf dem Bildschirm an. Informationen zur Ausgabe des Clients im Debugging-Modus finden Sie unter „Ausgabe eines DHCP-Client im Debugging-Modus“ auf Seite 486.

How to Run the DHCP Server in Debugging Mode

1 Melden Sie sich beim Serversystem als Superuser an.

2 Stoppen Sie den DHCP-Server vorübergehend.

```
# svcadm disable -t svc:/network/dhcp-server
```

Sie können den Server auch mit DHCP Manager oder dem Befehl `dhcpconfig` stoppen.

3 Starten Sie den Daemon im Debugging-Modus neu.

```
# /usr/lib/inet/in.dhcpd -d -v
```

Sie können auch eine der Befehlszeilenoptionen von `in.dhcpd` verwenden, die Sie normalerweise zum Ausführen des Daemon verwenden. Angenommen, Sie führen den Daemon als einen BOOTP-Relay-Agent aus, nehmen Sie die Option `-r` in den Befehl `in.dhcpd -d -v` auf.

Wenn der Daemon im Debugging-Modus ausgeführt wird, zeigt er während der Bearbeitung von DHCP- oder BOOTP-Anforderungen auf dem Bildschirm an. Informationen zur Ausgabe des Servers im Debugging-Modus finden Sie unter „Ausgabe eines DHCP-Servers im Debugging-Modus“ auf Seite 487.

So verwenden Sie `snoop` zur Überwachung des DHCP-Netzwerkverkehrs

1 Melden Sie sich als Superuser beim DHCP-Serversystem an.

2 Starten Sie den Befehl `snoop`, um die Aufzeichnung des Netzwerkverkehrs über die Netzwerkschnittstelle des Servers zu beginnen.

`# /usr/sbin/snoop -d` *interface* `-o` *snoop-output-filename* `udp port 67 or udp port 68`

Sie können z. B. den folgenden Befehl verwenden:

```
#  /usr/sbin/snoop -d hme0 -o /tmp/snoop.output udp port 67 or udp port 68
```

`snoop` setzt die Überwachung der Schnittstelle fort, bis Sie `snoop` durch Drücken von Strg-C beenden, nachdem Sie die erforderlichen Informationen gesammelt haben.

3 Booten Sie das Clientsystem, oder starten Sie den `dhcpagent`-Daemon auf dem Clientsystem neu.

„How to Run the DHCP Client in Debugging Mode“ auf Seite 484 beschreibt, wie `dhcpagent` neu gestartet wird.

4 Geben Sie den Befehl `snoop` auf dem Serversystem ein, um die Ausgabedatei mit dem Inhalt der Netzwerkpakete anzuzeigen:

`# /usr/sbin/snoop -i` *snoop-output-filename* `-x0 -v`

Sie können z. B. den folgenden Befehl verwenden:

```
# /usr/sbin/snoop -i /tmp/snoop.output -x0 -v
```

Siehe auch Informationen zur Interpretation der Ausgabe finden Sie unter „Ausgabe des DHCP-Befehls `snoop`“ auf Seite 490.

Ausgabe eines DHCP-Client im Debugging-Modus

Das folgende Beispiel zeigt die normale Ausgabe, wenn ein DHCP-Client im Debugging-Modus eine DHCP-Anforderung gesendet und die Konfigurationsinformationen von einem DHCP-Server erhält.

BEISPIEL 17–1 Normale Ausgabe eines DHCP-Client im Debugging-Modus

```
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhcpagent: debug: init_ifs: initted interface hme0
/sbin/dhcpagent: debug: insert_ifs: hme0: sdumax 1500, optmax 1260, hwtype 1, hwlen 6
/sbin/dhcpagent: debug: insert_ifs: inserted interface hme0
/sbin/dhcpagent: debug: register_acknak: registered acknak id 5
/sbin/dhcpagent: debug: unregister_acknak: unregistered acknak id 5
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x26018 (ARP reply filter)
/sbin/dhcpagent: info: setting IP netmask on hme0 to 255.255.192.0
/sbin/dhcpagent: info: setting IP address on hme0 to 10.23.3.233
/sbin/dhcpagent: info: setting broadcast address on hme0 to 10.23.63.255
/sbin/dhcpagent: info: added default router 10.23.0.1 on hme0
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x28054 (blackhole filter)
/sbin/dhcpagent: debug: configure_if: bound ifsp->if_sock_ip_fd
/sbin/dhcpagent: info: hme0 acquired lease, expires Tue Aug 10 16:18:33 2006
/sbin/dhcpagent: info: hme0 begins renewal at Tue Aug 10 15:49:44 2006
```

BEISPIEL 17–1 Normale Ausgabe eines DHCP-Client im Debugging-Modus *(Fortsetzung)*

```
/sbin/dhcpagent: info: hme0 begins rebinding at Tue Aug 10 16:11:03 2006
```

Kann der Client den DHCP-Server nicht erreichen, wird eventuell eine Ausgabe im Debugging-Modus angezeigt, die der im folgenden Beispiel ähnelt.

BEISPIEL 17–2 Ausgabe eines DHCP-Client in Debugging-Modus, die auf ein Problem hindeutet

```
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhcpagent: debug: init_ifs: initted interface hme0
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
```

Wenn diese Meldung angezeigt wird, hat die Client-Anforderung den Server nicht erreicht oder der Server kann keine Antwort an den Client senden. Führen Sie den Befehl `snoop` gemäß der Beschreibung unter „So verwenden Sie `snoop` zur Überwachung des DHCP-Netzwerkverkehrs“ auf Seite 485 auf dem Server aus, um festzustellen, ob Pakete vom Client den Server erreicht haben.

Ausgabe eines DHCP-Servers im Debugging-Modus

Die normale Ausgabe eines Servers im Debugging-Modus zeigt zunächst die Server-Konfigurationsinformationen an, denen nach dem Starten des Daemon Informationen zu den Netzwerkschnittstellen folgen. Nachdem der Daemon gestartet ist, zeigt die Ausgabe im Debugging-Modus Informationen zu Anforderungen an, die der Daemon verarbeitet. Beispiel 17–3 zeigt die Ausgabe eines DHCP-Servers im Debugging-Modus, der gerade gestartet wurde. Der Server verlängert das Leasing für einen Client, der eine Adresse verwendet, die einem anderen DHCP-Server gehört, der aber nicht antwortet.

BEISPIEL 17–3 Normale Ausgabe eines DHCP-Servers im Debugging-Modus

```
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: DHCP Server Mode.
Datastore: nisplus
Path: org_dir.dhcp.test..:dhcp.test..:$
DHCP offer TTL: 10
Ethers compatibility enabled.
BOOTP compatibility enabled.
ICMP validation timeout: 1000 milliseconds, Attempts: 2.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.21.255.255
Netmask: 255.255.0.0
Address: 10.21.0.2
```

BEISPIEL 17–3 Normale Ausgabe eines DHCP-Servers im Debugging-Modus *(Fortsetzung)*

```
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 10.22.255.255
Netmask: 255.255.0.0
Address: 10.22.0.1
Monitor (0007/qfe0) started...
Thread Id: 0007 - Monitoring Interface: qfe0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.23.63.255
Netmask: 255.255.192.0
Address: 10.23.0.1
Read 33 entries from DHCP macro database on Tue Aug 10 15:10:27 2006
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A maps to IP: 10.23.3.233
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
DHCP EXTEND 0934312543 0934316143 10.23.3.233 10.21.0.2
          0800201DBA3A SUNW.Ultra-5_10 0800201DBA3A
```

Beispiel 17–4 zeigte die Ausgabe eines DHCP-Daemon im Debugging-Modus, der als BOOTP-Relay-Agent gestartet wurde. Der Agent leitet Anforderungen von einem Client an einen DHCP-Server weiter, und leitet die Antworten des Servers an den Client.

BEISPIEL 17–4 Normale Ausgabe eines BOOTP-Relays im Debugging-Modus

```
Relay destination: 10.21.0.4 (blue-servr2)     network: 10.21.0.0
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: Relay Agent Mode.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.21.255.255
Netmask: 255.255.0.0
Address: 10.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 10.22.255.255
Netmask: 255.255.0.0
Address: 10.22.0.1
Monitor (0007/qfe0) started...
Thread Id: 0007 - Monitoring Interface: qfe0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.23.63.255
Netmask: 255.255.192.0
```

BEISPIEL 17–4 Normale Ausgabe eines BOOTP-Relays im Debugging-Modus *(Fortsetzung)*

```
Address: 10.23.0.1
Relaying request 0800201DBA3A to 10.21.0.4, server port.
BOOTP RELAY-SRVR 0934297685 0000000000 0.0.0.0 10.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 10.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
BOOTP RELAY-CLNT 0934297688 0000000000 10.23.0.1 10.23.3.233 0800201DBA3A
N/A 0800201DBA3A
Relaying request 0800201DBA3A to 10.21.0.4, server port.
BOOTP RELAY-SRVR 0934297689 0000000000 0.0.0.0 10.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 10.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
```

Falls ein Problem mit DHCP vorliegt, kann die Ausgabe im Debugging-Modus Anzeigewarnungen oder Fehlermeldungen enthalten. Suchen Sie mithilfe der folgenden Fehlermeldungsliste eines DHCP-Servers nach Lösungen.

`ICMP ECHO-Antwort an OFFER-Kandidat:` *IP-Adresse* `disabling`

Grund: Bevor der DHCP-Server dem Client eine IP-Adresse anbietet, sendet er einen ping-Befehl an die Adresse, um sicherzustellen, dass sie noch nicht verwendet wird. Wenn ein Client antwortet, wird die Adresse bereits verwendet.

Lösung: Stellen Sie sicher, dass die von Ihnen konfigurierten Adressen noch nicht verwendet werden. Dazu können Sie den `ping`-Befehl verwenden. Weitere Informationen finden Sie in der Manpage `ping`(1M).

`Keine weiteren IP-Adressen im Netzwerk` *Netzwerkadresse*`.`

Grund: In der DHCP-Netzwerktabelle, die dem Clientnetzwerk zugeordnet ist, stehen keine weiteren IP-Adressen mehr zur Verfügung.

Lösung: Weitere Adressen können Sie mit DHCP Manager oder dem Befehl `pntadm` erstellen. Wenn der DHCP-Daemon mehrere Teilnetze überwacht, achten Sie darauf, dass die zusätzlichen Adressen für das Teilnetz gelten, indem sich der Client befindet. Weitere Informationen finden Sie unter „Hinzufügen von IP-Adressen zum DHCP-Service“ auf Seite 406.

`Keine weiteren IP-Adressen für das Netzwerk` *Netzwerkadresse*`, wenn Sie den DHCP-Daemon im BOOTP-Kompatibilitätsmodus ausführen.`

Grund: BOOTP verwendet keine Leasing-Zeit, daher sucht der DHCP-Server nach freien Adressen mit gesetztem BOOTP-Flag, um BOOTP-Clients zuzuordnen.

Lösung: Verwenden Sie DHCP Manager zum Zuordnen von BOOTP-Adressen. Lesen Sie dazu „Unterstützen von BOOTP-Clients mit dem DHCP-Service (Übersicht der Schritte)“ auf Seite 399.

`Anforderung für den Zugriff auf nicht existierende Netzwerkdatenbank:` *Datenbankname* `im Datenspeicher:` *Datenspeicher*`.`

Grund: Während der Konfiguration des DHCP-Servers wurde für ein Teilnetz keine DHCP-Netzwerktabelle erstellt.

Lösung: Erstellen Sie die DHCP-Netzwerktabelle und neue IP-Adressen mit DHCP Manager oder dem Befehl `pntadm`. Lesen Sie dazu „Hinzufügen von DHCP-Netzwerken“ auf Seite 391.

`Es ist keine` *Tabellenname* `dhcp-Netzwerktabelle für das Netzwerk des DHCP-Client vorhanden.`

Grund: Während der Konfiguration des DHCP-Servers wurde für ein Teilnetz keine DHCP-Netzwerktabelle erstellt.

Lösung: Erstellen Sie die DHCP-Netzwerktabelle und neue IP-Adressen mit DHCP Manager oder dem Befehl `pntadm`. Lesen Sie dazu „Hinzufügen von DHCP-Netzwerken“ auf Seite 391.

`Client verwendet nicht-RFC1048 BOOTP-Cookie.`

Grund: Ein Gerät im Netzwerk versucht, auf eine nicht unterstützte Implementierung von BOOTP zuzugreifen.

Lösung: Ignorieren Sie diese Meldung, es sei denn, Sie müssen dieses Gerät konfigurieren. Wenn das Gerät unterstützt werden soll, finden Sie weitere Informationen unter „Unterstützen von BOOTP-Clients mit dem DHCP-Service (Übersicht der Schritte)“ auf Seite 399.

Ausgabe des DHCP-Befehls `snoop`

Aus der Ausgabe des Befehls `snoop` sollte hervorgehen, dass Datenpakete zwischen DHCP-Clientsystem und DHCP-Serversystem ausgetauscht wurden. In jedem Paket wird und die IP-Adresse jedes Systems angegeben. Ebenfalls enthalten sind die IP-Adressen für Router oder Relay-Agents im Pfad des Pakets. Wenn die Systeme keine Datenpakete austauschen, ist das Clientsystem eventuell nicht in der Lage, das Serversystem zu kontaktieren. Das Problem liegt dann auf einen niedrigen Ebene.

Um die Ausgabe des Befehls `snoop` zu bewerten, müssen Sie das erwartete Verhalten kennen. Beispielsweise müssen Sie wissen, ob die Anforderung über einen BOOTP-Relay-Agent erfolgt. Außerdem müssen Sie die MAC-Adressen und die IP-Adresse der am Datenaustausch beteiligten Systeme kennen, so dass Sie feststellen können, ob die angezeigten Werte korrekt sind. Falls mehrere Netzwerkschnittstellen vorhanden sind, müssen Sie auch die Adressen dieser Netzwerkschnittstellen kennen.

Das folgende Beispiel zeigt eine normale Ausgabe des Befehls `snoop` für eine DHCP-Bestätigungsnachricht, die vom DHCP-Server auf `blue-servr2` an einen Client mit der MAC-Adresse `8:0:20:8e:f3:7e` gesendet wurde. In dieser Nachricht weist der Server dem Client die IP-Adresse `192.168.252.6` und den Hostnamen `white-6` zu. Darüber hinaus enthält die Meldung verschiedene standardmäßige Netzwerkoptionen und einige Hersteller-spezifische Optionen für den Client.

BEISPIEL 17–5 Beispielausgabe des Befehls `snoop` für ein Paket

```
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 26 arrived at 14:43:19.14
ETHER:  Packet size = 540 bytes
ETHER:  Destination = 8:0:20:8e:f3:7e, Sun
ETHER:  Source      = 8:0:20:1e:31:c1, Sun
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 526 bytes
IP:   Identification = 64667
IP:   Flags = 0x4 IP:         .1.. .... = do not fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 254 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 157a
IP:   Source address = 10.21.0.4, blue-servr2
IP:   Destination address = 192.168.252.6, white-6
IP:   No options
IP:   UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 67
UDP:  Destination port = 68 (BOOTPC)
UDP:  Length = 506
UDP:  Checksum = 5D4C
UDP:
DHCP: ----- Dynamic Host Configuration Protocol -----
DHCP:
DHCP: Hardware address type (htype) =  1 (Ethernet (10Mb))
DHCP: Hardware address length (hlen) = 6 octets
DHCP: Relay agent hops = 0
DHCP: Transaction ID = 0x2e210f17
DHCP: Time since boot = 0 seconds
DHCP: Flags = 0x0000
DHCP: Client address (ciaddr) = 0.0.0.0
DHCP: Your client address (yiaddr) = 192.168.252.6
DHCP: Next server address (siaddr) = 10.21.0.2
DHCP: Relay agent address (giaddr) = 0.0.0.0
DHCP: Client hardware address (chaddr) = 08:00:20:11:E0:1B
```

BEISPIEL 17–5 Beispielausgabe des Befehls snoop für ein Paket *(Fortsetzung)*

```
DHCP:
DHCP: ----- (Options) field options -----
DHCP:
DHCP: Message type = DHCPACK
DHCP: DHCP Server Identifier = 10.21.0.4
DHCP: Subnet Mask = 255.255.255.0
DHCP: Router at = 192.168.252.1
DHCP: Broadcast Address = 192.168.252.255
DHCP: NISPLUS Domainname = dhcp.test
DHCP: IP Address Lease Time = 3600 seconds
DHCP: UTC Time Offset = -14400 seconds
DHCP: RFC868 Time Servers at = 10.21.0.4
DHCP: DNS Domain Name = sem.example.com
DHCP: DNS Servers at = 10.21.0.1
DHCP: Client Hostname = white-6
DHCP: Vendor-specific Options (166 total octets):
DHCP:   (02) 04 octets  0x8194AE1B (unprintable)
DHCP:   (03) 08 octets  "pacific"
DHCP:   (10) 04 octets  0x8194AE1B (unprintable)
DHCP:   (11) 08 octets  "pacific"
DHCP:   (15) 05 octets  "xterm"
DHCP:   (04) 53 octets  "/export/s2/base.s2s/latest/Solaris_8/Tools/Boot"
DHCP:   (12) 32 octets  "/export/s2/base.s2s/latest"
DHCP:   (07) 27 octets  "/platform/sun4u/kernel/unix"
DHCP:   (08) 07 octets  "EST5EDT"
  0: 0800 208e f37e 0800 201e 31c1 0800 4500    .. .ó~.. .1...E.
 16: 020e fc9b 4000 fe11 157a ac15 0004 c0a8    ....@....z......
 32: fc06 0043 0044 01fa 5d4c 0201 0600 2e21    ...C.D..]L.....!
 48: 0f17 0000 0000 0000 0000 c0a8 fc06 ac15    ...............
 64: 0002 0000 0000 0800 2011 e01b 0000 0000    ........ .......
 80: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
 96: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
112: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
128: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
144: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
160: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
176: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
192: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
208: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
224: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
240: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
256: 0000 0000 0000 0000 0000 0000 0000 0000    ...............
272: 0000 0000 0000 6382 5363 3501 0536 04ac    ......c.Sc5..6..
288: 1500 0401 04ff ffff 0003 04c0 a8fc 011c    ...............
304: 04c0 a8fc ff40 0964 6863 702e 7465 7374    .....@.dhcp.test
320: 3304 0000 0e10 0204 ffff c7c0 0404 ac15    3..............
336: 0004 0f10 736e 742e 6561 7374 2e73 756e    ....sem.example.
352: 2e63 6f6d 0604 ac15 0001 0c07 7768 6974    com.........whit
368: 652d 362b a602 0481 94ae 1b03 0861 746c    e-6+.........pac
384: 616e 7469 630a 0481 94ae 1b0b 0861 746c    ific.........pac
400: 616e 7469 630f 0578 7465 726d 0435 2f65    ific...xterm.5/e
416: 7870 6f72 742f 7332 382f 6261 7365 2e73    xport/sx2/bcvf.s
432: 3238 735f 776f 732f 6c61 7465 7374 2f53    2xs_btf/latest/S
448: 6f6c 6172 6973 5f38 2f54 6f6f 6c73 2f42    olaris_x/Tools/B
464: 6f6f 740c 202f 6578 706f 7274 2f73 3238    oot. /export/s2x
480: 2f62 6173 652e 7332 3873 5f77 6f73 2f6c    /bcvf.s2xs_btf/l
```

BEISPIEL 17–5 Beispielausgabe des Befehls snoop für ein Paket *(Fortsetzung)*

```
496: 6174 6573 7407 1b2f 706c 6174 666f 726d    atest../platform
512: 2f73 756e 346d 2f6b 6572 6e65 6c2f 756e    /sun4u/kernel/un
528: 6978 0807 4553 5435 4544 54ff              ix..EST5EDT.
```

Problems With Inaccurate DHCP Configuration Information

Wenn ein DHCP-Client ungenaue Informationen in seinen Netzwerkkonfigurationsinformationen erhält, müssen Sie die DHCP-Serverdaten prüfen. Achten Sie dabei auf die Optionswerte in den Makros, die der DHCP-Server für diesen Client verarbeitet. Beispiele für ungenaue Informationen könnten ein falscher NIS-Domänenname oder eine falsche Router-IP-Adresse sein.

Die folgenden allgemeinen Richtlinien helfen Ihnen dabei, die Quelle der ungenauen Informationen festzustellen:

- Prüfen Sie die Makros, die nach der Beschreibung unter „So zeigen Sie die auf einem DHCP-Server definierten Makros an (DHCP Manager)“ auf Seite 421 auf dem Server definiert wurden. Lesen Sie die Informationen unter „Reihenfolge der Makroverarbeitung“ auf Seite 335, und stellen Sie fest, welche Makros automatisch für diesen Client verarbeitet werden.
- Prüfen Sie die Netzwerktabelle, um festzustellen, welches Makro (sofern vorhanden) der IP-Adresse des Clients als Konfigurationsmakro zugeordnet ist. Weitere Informationen finden Sie unter „Arbeiten mit IP-Adressen im DHCP-Service (Übersicht der Schritte)“ auf Seite 402.
- Achten Sie auf Optionen, die in mehreren Makros erscheinen. Achten Sie darauf, dass der Wert, den die Option annehmen soll, im zuletzt verarbeiteten Makro korrekt eingerichtet ist.
- Nehmen Sie eventuell Änderungen an dem betreffenden Makro vor, um sicherzustellen, dass der korrekte Wert an den Client übergeben wird. Lesen Sie dazu „Ändern von DHCP-Makros“ auf Seite 422.

Probleme mit dem vom DHCP-Client angegebenen Hostnamen

In diesem Abschnitt werden Probleme beschrieben, die eventuell bei DHCP-Clients auftreten, die ihre eigenen Hostnamen bei DNS registrieren.

DHCP-Client fordert keinen Hostnamen an

Handelt es sich bei Ihrem Client nicht um einen Oracle Solaris DHCP-Client, suchen Sie in der Dokumentation für Ihren DHCP-Client nach Informationen, wie der Client so konfiguriert wird, dass er einen Hostnamen anfordert. Bei Oracle Solaris DHCP-Clients lesen Sie „So konfigurieren Sie einen Oracle Solaris DHCPv4-Client zur Anforderung eines bestimmten Hostnamens“ auf Seite 468.

DHCP-Client erhält den angeforderten Hostnamen nicht

In der folgenden Liste sind mögliche Probleme beschrieben, die dazu führen könnten, dass ein Client den angeforderten Hostnamen nicht erhält. Weiterhin werden Lösungsvorschläge angeboten.

Problem: Client akzeptiert ein Angebot von einem DHCP-Server, der keine DNS-Aktualisierungen ausgibt.

Lösung: Wenn dem Client zwei DHCP-Server zur Verfügung stehen, sollten beide Server so konfiguriert sein, dass sie DNS-Aktualisierungen bereitstellen können. Informationen zur Konfiguration von DHCP-Server und DNS-Server finden Sie unter „Aktivieren von dynamischen DNS-Aktualisierungen durch einen DHCP-Server“ auf Seite 382.

So können Sie feststellen, ob der DHCP-Server so konfiguriert ist, dass er DNS-Aktualisierungen bereitstellt:

1. Ermitteln Sie die IP-Adresse des DHCP-Servers des Client. Geben Sie auf dem Clientsystem den Befehl `snoop` ein oder rufen Sie eine andere Anwendung zur Erfassung von Netzwerkpaketen auf. Lesen Sie „So verwenden Sie `snoop` zur Überwachung des DHCP-Netzwerkverkehrs“ auf Seite 485 und führen Sie das Verfahren auf dem Client noch einmal durch. Suchen Sie in der Ausgabe des Befehls `snoop` nach dem Bezeichner des DHCP-Servers, um die IP-Adresse des Servers in Erfahrung zu bringen.
2. Melden Sie sich beim DHCP-Serversystem an, um sicherzustellen, dass dieses System so konfiguriert ist, dass es DNS-Aktualisierungen durchführen kann. Melden Sie sich als Superuser an, und geben Sie den folgenden Befehl ein:

   `dhcpconfig -P`

   Wenn `UPDATE_TIMEOUT` als ein Serverparameter aufgeführt ist, wurde der DHCP-Server so konfiguriert, dass er DNS-Aktualisierungen durchführen kann.
3. Prüfen Sie die `/etc/named.conf`-Datei auf dem DNS-Server. Suchen Sie nach dem Schlüsselwort `allow-update` im Bereich `zone` der entsprechenden Domäne. Wenn der Server DNS-Aktualisierungen durch den DHCP-Server gestattet, ist die IP-Adresse des DHCP-Servers für das Schlüsselwort `allow-update` enthalten.

Problem: Client verwendet die Option FQDN, um den Hostnamen anzugeben. Oracle Solaris DHCP unterstützt die Option FQDN derzeit nicht, weil sie offiziell nicht zum DHCP-Protokoll gehört.

Lösung: Geben Sie auf dem Server den Befehl snoop ein oder rufen Sie eine andere Anwendung zur Erfassung von Netzwerkpaketen auf. Lesen Sie dazu „So verwenden Sie snoop zur Überwachung des DHCP-Netzwerkverkehrs" auf Seite 485. Suchen Sie in der Ausgabe des Befehls snoop nach der Option FQDN in einem Paket von Client.

Konfigurieren Sie den Client so, dass er den Hostnamen mit der Option Hostname angibt. Hostname hat den Optionscode 12. Anweisungen finden Sie in der Client-Dokumentation.

Bei einem Oracle Solaris-Client lesen Sie „So konfigurieren Sie einen Oracle Solaris DHCPv4-Client zur Anforderung eines bestimmten Hostnamens" auf Seite 468

Problem: Der DHCP-Server, der dem Client eine Adresse anbietet, kennt die DNS-Domäne des Clients nicht.

Lösung: Prüfen Sie auf dem DHCP-Server, ob die Option DNSdmain einen gültigen Wert aufweist. Setzen Sie die Option DNSdmain in einem Makro, das für diesen Client verwendet wird, auf dem korrekten DNS-Domänennamen. DNSdmain ist im Allgemeinen im Netzwerkmakro enthalten. Informationen zum Ändern von Optionswerten in einem Makro finden Sie unter „Ändern von DHCP-Makros" auf Seite 422.

Problem: Der von einem Client angeforderte Hostname entspricht einer IP-Adresse, die nicht von diesem DHCP-Server verwaltet wird. Der Oracle Solaris DHCP-Server führt keine DNS-Aktualisierungen für IP-Adressen durch, die der Server nicht verwaltet.

Lösung: Achten Sie im syslog auf eine der folgenden Meldungen vom DHCP-Server:

- Es ist keine *n.n.n.n* dhcp-Netzwerktabelle für das Netzwerk des DHCP-Client vorhanden.
- DHCP-Netzwerkdatensatz für *n.n.n.n* ist nicht verfügbar. Anforderung wird ignoriert.

Konfigurieren Sie den Client so, dass er einen anderen Namen anfordert. Lesen Sie dazu „So konfigurieren Sie einen Oracle Solaris DHCPv4-Client zur Anforderung eines bestimmten Hostnamens" auf Seite 468. Wählen Sie einen Namen, der eine von diesem DHCP-Server verwaltete Adresse zugeordnet ist. Die Adressenzuordnungen können Sie der Registerkarte „Adressen" in DHCP Manager entnehmen. Alternativ wählen Sie eine Adresse, die keiner IP-Adresse zugeordnet ist.

Problem: Der von einem Client angeforderte Hostname entspricht einer IP-Adresse, die derzeit nicht zur Verfügung steht. Die Adresse wird eventuell schon verwendet, ist in einem Leasing an einen anderen Client vergeben oder wird einem anderen Client angeboten.

Lösung: Achten Sie im syslog auf die folgende Meldung vom the DHCP-Server: ICMP ECHO reply to OFFER candidate: *n.n.n.n*.

Konfigurieren Sie den Client so, dass er einen Namen wählt, der einer anderen IP-Adresse entspricht. Alternativ fordern Sie die Adresse von dem Client zurück, der die Adresse momentan verwendet.

Problem: DNS-Server ist so konfiguriert, dass er keine Aktualisierungen vom DHCP-Server akzeptiert.

Lösung: Prüfen Sie die `/etc/named.conf`-Datei auf dem DNS-Server. Suchen Sie nach der IP-Adresse des DHCP-Servers mit dem `allow-update`-Schlüsselwort im entsprechenden `zone`-Bereich für die Domäne des DHCP-Servers. Ist diese IP-Adresse nicht vorhanden, wurde der DNS-Server so konfiguriert, dass er keine Aktualisierungen vom DHCP-Server akzeptiert.

Informationen zur Konfiguration des DNS-Servers finden Sie unter „So aktivieren Sie die dynamische DNS-Aktualisierung für DHCP-Clients“ auf Seite 383.

Verfügt der DHCP-Server über mehrere Schnittstellen, müssen Sie den DNS-Server eventuell so konfigurieren, dass er Aktualisierungen von allen Adressen des DHCP-Servers akzeptiert. Aktivieren Sie das Debugging auf den DNS-Server, um festzustellen, ob die Aktualisierungen den DNS-Server erreichen. Wenn der DNS-Server Aktualisierungsanforderungen empfängt, prüfen Sie die Ausgabe im Debugging-Modus, um festzustellen, warum die Aktualisierungen nicht stattgefunden haben. Informationen zum DNS-Debugging-Modus finden Sie in der Manpage `in.named.1M`.

Problem: DNS-Aktualisierungen wurden im zugewiesenen Zeitraum nicht vollständig abgeschlossen. DHCP-Server haben keine Hostnamen an Clients zurückgegeben, wenn die DNS-Aktualisierungen nicht im konfigurierten Zeitrahmen abgeschlossen wurden. Versuche zum Vervollständigen der DNS-Aktualisierungen werden jedoch fortgesetzt.

Lösung: Geben Sie den Befehl `nslookup` ein, um festzustellen, ob die Aktualisierungen erfolgreich abgeschlossen wurden. Weitere Informationen finden Sie in der Manpage `nslookup`(1M).

Angenommen, die DNS-Domäne ist `hills.example.org` und die IP-Adresse des DNS-Servers lautet `10.76.178.11`. Der Hostname, den der Client registrieren möchte, lautet `cathedral`. Mit dem folgenden Befehle können Sie feststellen, ob `cathedral` bei diesem DNS-Server registriert wurde :

```
nslookup cathedral.hills.example.org 10.76.178.11
```

Wenn die Aktualisierung erfolgreich abgeschlossen wurde, jedoch nicht in der zugewiesenen Zeit, müssen Sie den Timeout-Wert erhöhen. Lesen Sie dazu „So aktivieren Sie die dynamische DNS-Aktualisierung für DHCP-Clients“ auf Seite 383. In diesem Verfahren geben Sie in Sekunden an, wie lange auf eine Antwort vom DNS-Server gewartet werden soll, bevor eine Zeitüberschreitung eintritt.

KAPITEL 18

DHCP – Befehle und Dateien (Referenz)

In diesem Kapitel werden die Beziehungen zwischen DHCP-Befehlen und DHCP-Dateien beschrieben. Die Verwendung der Befehle wird in diesem Kapitel nicht erklärt.

Dieses Kapitel enthält die folgenden Informationen:

- „DHCP-Befehle“ auf Seite 497
- „Vom DHCP-Service verwendete Dateien“ auf Seite 504
- „DHCP-Optionsinformationen“ auf Seite 506

DHCP-Befehle

In der folgenden Tabelle sind die Befehle aufgelistet, die Sie zur Verwaltung von DHCP in Ihrem Netzwerk verwenden können.

TABELLE 18–1 In DHCP verwendete Befehle

Befehl	Beschreibung	Manpage
`dhtadm`	Mit diesem Befehl nehmen Sie Änderungen an den Optionen und Makros in der `dhcptab`-Tabelle vor. Dieser Befehl eignet sich in Skripten, mit denen Sie Änderungen an Ihren DHCP-Informationen automatisieren. Verwenden Sie den Befehl `dhtadm` mit der Option `-P`, und leiten Sie die Ausgabe über den Befehl `grep`, um schnell nach bestimmten Optionswerten in der Tabelle `dhcptab` suchen zu können.	`dhtadm`(1M)
`pntadm`	Mit diesem Befehl nehmen Sie Änderungen an den DHCP-Netzwerktabellen vor, die Client-IDs zu IP-Adressen zuordnen und optional Konfigurationsinformationen mit IP-Adressen verbinden.	`pntadm`(1M)
`dhcpconfig`	Mit diesem Befehl konfigurieren und dekonfigurieren Sie DHCP-Server und BOOTP-Relay-Agents. Darüber hinaus dient dieser Befehl zum Konvertieren in ein anderes Datenspeicherformat sowie zum Importieren und Exportieren von DHCP-Konfigurationsdateien.	`dhcpconfig`(1M)

TABELLE 18–1 In DHCP verwendete Befehle *(Fortsetzung)*

Befehl	Beschreibung	Manpage
`in.dhcpd`	Der DHCP-Server-Daemon. Der Daemon startet, wenn das System hochgefahren wird. Der Server-Daemon darf nicht direkt gestartet werden. Zum Starten und Stoppen des Daemon verwenden Sie DHCP Manager, den Befehl `svcadm` oder `dhcpconfig`. Der Daemon darf nur direkt aufgerufen werden, um den Server im Debugging-Modus auszuführen, so dass Probleme behoben werden können.	`in.dhcpd`(1M)
`dhcpmgr`	Der DHCP Manager ist ein Tool mit einer grafischen Benutzeroberfläche (GUI), mit dem Sie den DHCP-Service konfigurieren und verwalten. DHCP Manager ist das von Oracle Solaris empfohlene DHCP-Verwaltungstool.	`dhcpmgr`(1M)
`ifconfig`	Dieser Befehl wird beim Booten des Systems verwendet, um Netzwerkschnittstellen IP-Adressen zuzuordnen, Netzwerkschnittstellenparameter zu konfigurieren oder beides. Auf einem Oracle Solaris DHCP-Client startet `ifconfig` DHCP, um die zur Konfiguration einer Netzwerkschnittstelle erforderlichen Parameter zu beziehen (einschließlich der IP-Adresse).	`ifconfig`(1M)
`dhcpinfo`	Dieser Befehl wird von System-Startskripten auf Oracle Solaris-Clientsystemen verwendet, um Informationen vom DHCP-Client-Daemon `dhcpagent` zu beziehen (z. B. den Hostnamen). Sie können `dhcpinfo` auch in Skripten oder an der Befehlszeile verwenden, um bestimmte Parameterwerte zu beziehen.	`dhcpinfo`(1)
`snoop`	Dient zum Erfassen und Anzeigen der Inhalte von Datenpaketen, die im Netzwerk ausgetauscht werden. `snoop` eignet sich insbesondere zur Fehlersuche bei Problemen mit dem DHCP-Service.	`snoop`(1M)
`dhcpagent`	Der DHCP-Client-Daemon, der die Client-Seite des DHCP-Protokolls implementiert.	`dhcpagent`(1M)

Ausführen von DHCP-Befehlen in Skripten

Die Befehle `dhcpconfig`, `dhtadm` und `pntadm` wurden zur Verwendung in Skripten optimiert. So eignet sich der Befehl `pntadm` insbesonders zum Erstellen zahlreicher IP-Adresseinträge in einer DHCP-Netzwerktabelle. Im folgenden Beispielskript wird der Befehl `pntadm` dazu verwendet, IP-Adressen im Batch-Modus zu erzeugen.

BEISPIEL 18–1 `addclient.ksh`-Skript mit dem Befehl `pntadm`

```
#! /usr/bin/ksh
#
# This script utilizes the pntadm batch facility to add client entries
# to a DHCP network table. It assumes that the user has the rights to
# run pntadm to add entries to DHCP network tables.

#
```

BEISPIEL 18–1 `addclient.ksh`-Skript mit dem Befehl `pntadm` *(Fortsetzung)*

```
# Based on the nsswitch setting, query the netmasks table for a netmask.
# Accepts one argument, a dotted IP address.
#
get_netmask()
{
    MTMP=‘getent netmasks ${1} | awk ’{ print $2 }’‘
    if [ ! -z "${MTMP}" ]
    then
        print - ${MTMP}
    fi
}

#
# Based on the network specification, determine whether or not network is
# subnetted or supernetted.
# Given a dotted IP network number, convert it to the default class
# network.(used to detect subnetting). Requires one argument, the
# network number. (e.g. 10.0.0.0) Echos the default network and default
# mask for success, null if error.
#
get_default_class()
{
    NN01=${1%%.*}
    tmp=${1#*.}
    NN02=${tmp%%.*}
    tmp=${tmp#*.}
    NN03=${tmp%%.*}
    tmp=${tmp#*.}
    NN04=${tmp%%.*}
    RETNET=""
    RETMASK=""

    typeset -i16 ONE=10#${1%%.*}
    typeset -i10 X=$((${ONE}&16#f0))
    if [ ${X} -eq 224 ]
    then
        # Multicast
        typeset -i10 TMP=$((${ONE}&16#f0))
        RETNET="${TMP}.0.0.0"
        RETMASK="240.0.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#80))
    if [ -z "${RETNET}" -a ${X} -eq 0 ]
    then
        # Class A
        RETNET="${NN01}.0.0.0"
        RETMASK="255.0.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#c0))
    if [ -z "${RETNET}" -a ${X} -eq 128 ]
    then
        # Class B
        RETNET="${NN01}.${NN02}.0.0"
        RETMASK="255.255.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#e0))
```

BEISPIEL 18–1 `addclient.ksh`-Skript mit dem Befehl `pntadm` *(Fortsetzung)*

```
    if [ -z "${RETNET}" -a ${X} -eq 192 ]
    then
        # Class C
        RETNET="${NN01}.${NN02}.${NN03}.0"
        RETMASK="255.255.255.0"
    fi
    print - ${RETNET} ${RETMASK}
    unset NNO1 NNO2 NNO3 NNO4 RETNET RETMASK X ONE
}

#
# Given a dotted form of an IP address, convert it to its hex equivalent.
#
convert_dotted_to_hex()
{
    typeset -i10 one=${1%%.*}
    typeset -i16 one=${one}
    typeset -Z2 one=${one}
    tmp=${1#*.}

    typeset -i10 two=${tmp%%.*}
    typeset -i16 two=${two}
    typeset -Z2 two=${two}
    tmp=${tmp#*.}

    typeset -i10 three=${tmp%%.*}
    typeset -i16 three=${three}
    typeset -Z2 three=${three}
    tmp=${tmp#*.}

    typeset -i10 four=${tmp%%.*}
    typeset -i16 four=${four}
    typeset -Z2 four=${four}

     hex=‘print - ${one}${two}${three}${four} | sed -e ’s/#/0/g’‘
     print - 16#${hex}
     unset one two three four tmp
}

#
# Generate an IP address given the network address, mask, increment.
#
get_addr()
{
    typeset -i16 net=‘convert_dotted_to_hex ${1}‘
    typeset -i16 mask=‘convert_dotted_to_hex ${2}‘
    typeset -i16 incr=10#${3}

    # Maximum legal value - invert the mask, add to net.
    typeset -i16 mhosts=~${mask}
    typeset -i16 maxnet=${net}+${mhosts}

    # Add the incr value.
    let net=${net}+${incr}

    if [ $((${net} < ${maxnet})) -eq 1 ]
```

BEISPIEL 18–1 `addclient.ksh`-Skript mit dem Befehl `pntadm` *(Fortsetzung)*

```
    then
        typeset -i16 a=${net}\&16#ff000000
        typeset -i10 a="${a}>>24"

        typeset -i16 b=${net}\&16#ff0000
        typeset -i10 b="${b}>>16"

        typeset -i16 c=${net}\&16#ff00
        typeset -i10 c="${c}>>8"

        typeset -i10 d=${net}\&16#ff
        print - "${a}.${b}.${c}.${d}"
    fi
    unset net mask incr mhosts maxnet a b c d
}

# Given a network address and client address, return the index.
client_index()
{
    typeset -i NNO1=${1%%.*}
    tmp=${1#*.}
    typeset -i NNO2=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO3=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO4=${tmp%%.*}

    typeset -i16 NNF1
    let NNF1=${NNO1}
    typeset -i16 NNF2
    let NNF2=${NNO2}
    typeset -i16 NNF3
    let NNF3=${NNO3}
    typeset -i16 NNF4
    let NNF4=${NNO4}
    typeset +i16 NNF1
    typeset +i16 NNF2
    typeset +i16 NNF3
    typeset +i16 NNF4
    NNF1=${NNF1#16\#}
    NNF2=${NNF2#16\#}
    NNF3=${NNF3#16\#}
    NNF4=${NNF4#16\#}
    if [ ${#NNF1} -eq 1 ]
    then
        NNF1="0${NNF1}"
    fi
    if [ ${#NNF2} -eq 1 ]
    then
        NNF2="0${NNF2}"
    fi
    if [ ${#NNF3} -eq 1 ]
    then
        NNF3="0${NNF3}"
    fi
    if [ ${#NNF4} -eq 1 ]
```

BEISPIEL 18–1 `addclient.ksh`-Skript mit dem Befehl `pntadm` *(Fortsetzung)*

```
    then
        NNF4="0${NNF4}"
    fi
    typeset -i16 NN
    let NN=16#${NNF1}${NNF2}${NNF3}${NNF4}
    unset NNF1 NNF2 NNF3 NNF4

    typeset -i NNO1=${2%%.*}
    tmp=${2#*.}
    typeset -i NNO2=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO3=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO4=${tmp%%.*}
    typeset -i16 NNF1
    let NNF1=${NNO1}
    typeset -i16 NNF2
    let NNF2=${NNO2}
    typeset -i16 NNF3
    let NNF3=${NNO3}
    typeset -i16 NNF4
    let NNF4=${NNO4}
    typeset +i16 NNF1
    typeset +i16 NNF2
    typeset +i16 NNF3
    typeset +i16 NNF4
    NNF1=${NNF1#16\#}
    NNF2=${NNF2#16\#}
    NNF3=${NNF3#16\#}
    NNF4=${NNF4#16\#}
    if [ ${#NNF1} -eq 1 ]
    then
        NNF1="0${NNF1}"
    fi
    if [ ${#NNF2} -eq 1 ]
    then
        NNF2="0${NNF2}"
    fi
    if [ ${#NNF3} -eq 1 ]
    then
        NNF3="0${NNF3}"
    fi
    if [ ${#NNF4} -eq 1 ]
    then
        NNF4="0${NNF4}"
    fi
    typeset -i16 NC
    let NC=16#${NNF1}${NNF2}${NNF3}${NNF4}
    typeset -i10 ANS
    let ANS=${NC}-${NN}
    print - $ANS
}

#
# Check usage.
#
```

BEISPIEL 18–1 `addclient.ksh`-Skript mit dem Befehl `pntadm` *(Fortsetzung)*

```
if [ "$#" != 3 ]
then
    print "This script is used to add client entries to a DHCP network"
    print "table by utilizing the pntadm batch facilty.\n"
    print "usage: $0 network start_ip entries\n"
    print "where: network is the IP address of the network"
        print "       start_ip is the starting IP address \n"
        print "       entries is the number of the entries to add\n"
    print "example: $0 10.148.174.0 10.148.174.1 254\n"
    return
fi

#
# Use input arguments to set script variables.
#
NETWORK=$1
START_IP=$2
typeset -i STRTNUM=`client_index ${NETWORK} ${START_IP}`
let ENDNUM=${STRTNUM}+$3
let ENTRYNUM=${STRTNUM}
BATCHFILE=/tmp/batchfile.$$
MACRO=`uname -n`

#
# Check if mask in netmasks table. First try
# for network address as given, in case VLSM
# is in use.
#
NETMASK=`get_netmask ${NETWORK}`
if [ -z "${NETMASK}" ]
then
    get_default_class ${NETWORK} | read DEFNET DEFMASK
    # use the default.
    if [ "${DEFNET}" != "${NETWORK}" ]
    then
        # likely subnetted/supernetted.
        print - "\n\n###\tWarning\t###\n"
        print - "Network ${NETWORK} is netmasked, but no entry was found  \n
              in the 'netmasks' table; please update the 'netmasks'  \n
              table in the appropriate nameservice before continuing. \n
              (See /etc/nsswitch.conf.) \n" >&2
        return 1
    else
        # use the default.
        NETMASK="${DEFMASK}"
    fi
fi

#
# Create a batch file.
#
print -n "Creating batch file "
while [ ${ENTRYNUM} -lt ${ENDNUM} ]
do
    if [ $((${ENTRYNUM}-${STRTNUM}))%50 -eq 0 ]
    then
```

BEISPIEL 18–1 `addclient.ksh`-Skript mit dem Befehl `pntadm` *(Fortsetzung)*

```
        print -n "."
    fi

    CLIENTIP=‘get_addr ${NETWORK} ${NETMASK} ${ENTRYNUM}‘
    print "pntadm -A ${CLIENTIP} -m ${MACRO} ${NETWORK}" >> ${BATCHFILE}
    let ENTRYNUM=${ENTRYNUM}+1
done
print " done.\n"

#
# Run pntadm in batch mode and redirect output to a temporary file.
# Progress can be monitored by using the output file.
#
print "Batch processing output redirected to ${BATCHFILE}"
print "Batch processing started."

pntadm -B ${BATCHFILE} -v > /tmp/batch.out 2 >&1

print "Batch processing completed."
```

Vom DHCP-Service verwendete Dateien

In der folgenden Tabelle sind die Oracle Solaris DHCP zugeordneten Dateien aufgeführt.

TABELLE 18–2 Von DHCP-Daemons und -Befehlen verwendete Dateien und Tabellen

Datei- oder Tabellenname	Beschreibung	Manpage
`dhcptab`	Ein allgemeiner Begriff für die Tabelle der DHCP-Konfigurationsinformationen, die als Optionen mit zugewiesenen Werten aufgezeichnet und dann in Makros gruppiert werden. Der Name der `dhcptab`-Tabelle und ihr Speicherort wird durch den Datenspeicher bestimmt, den Sie für Ihre DHCP-Informationen verwenden.	`dhcptab`(4)
DHCP-Netzwerktabelle	Ordnet IP-Adressen zu Client-IDs und Konfigurationsoptionen zu. DHCP-Netzwerktabellen werden nach der IP-Adresse des Netzwerks benannt, z. B. `10.21.32.0`. Es gibt keine Datei mit dem Namen `dhcp_Netzwerk`. Name und Speicherort der DHCP-Netzwerktabellen wird durch den Datenspeicher bestimmt, den Sie für Ihre DHCP-Informationen verwenden.	`dhcp_network`(4)
`dhcpsvc.conf`	Speichert Startoptionen für den DHCP-Daemon und Datenspeicherinformationen. Diese Datei darf nicht manuell bearbeitet werden. Zum Ändern der Startoptionen verwenden Sie den Befehl `dhcpconfig`.	`dhcpsvc.conf`(4)

TABELLE 18–2 Von DHCP-Daemons und -Befehlen verwendete Dateien und Tabellen *(Fortsetzung)*

Datei- oder Tabellenname	Beschreibung	Manpage
`nsswitch.conf`	Gibt den Speicherort der Namen-Service-Datenbanken und die Reihenfolge an, in der die Namen-Services für verschiedene Informationsarten verwendet werden. In der Datei `nsswitch.conf` werden genau die Konfigurationsinformationen gespeichert, die Sie zur Konfiguration eines DHCP-Servers benötigen. Die Datei befindet sich in dem Verzeichnis `/etc`.	`nsswitch.conf(4)`
`resolv.conf`	Enthält Informationen, die zum Auflösen von DNS-Anfragen verwendet werden. Aus dieser Datei werden während der Konfiguration des DHCP-Servers Informationen zur DNS-Domäne und DNS-Server bezogen. Die Datei befindet sich in dem Verzeichnis `/etc`.	`resolv.conf(4)`
`dhcp.`*Schnittstelle*	Kennzeichnet, dass DHCP auf der Netzwerkschnittstelle des Client verwendet wird, die in dem Dateinamen `dhcp.`*Schnittstelle* angegeben ist. Beispielsweise gibt das Vorhandensein der Datei `dhcp.qe0` an, das DHCP auf der Schnittstelle namens `qe0` verwendet wird. Die `dhcp.`*Schnittstelle*-Datei kann Befehle enthalten, die als Optionen an den `ifconfig`-Befehl übergeben werden, der zum Starten von DHCP auf dem Client verwendet wird. Die Datei befindet sich im Verzeichnis `/etc` auf den Oracle Solaris DHCP-Clientsystemen.	Keine bestimmte Manpage, siehe `dhcp(5)`
Schnittstelle`.dhc`	Enthält die Konfigurationsparameter, die von DHCP für eine bestimmte Netzwerkschnittstelle bezogen werden. Der Client speichert die aktuellen Konfigurationsinformationen in `/etc/dhcp/`*Schnittstelle*`.dhc` zwischen, wenn das Leasing IP-Adresse der Schnittstelle abgelaufen ist. Angenommen, DHCP wird auf der Schnittstelle `qe0` verwendet, so speichert der `dhcpagent` die Konfigurationsinformationen in `/etc/dhcp/qe0.dhc` zwischen. Wenn DHCP das nächste Mal auf der Schnittstelle gestartet wird, fordert der Client die zwischengespeicherte Konfiguration an, sofern dieses Leasing noch nicht abgelaufen ist. Wenn der DHCP-Server die Anforderung verweigert, beginnt der Client den standardmäßigen Prozess zur Aushandlung eines DHCP-Leasing.	Keine bestimmte Manpage, siehe `dhcpagent(1M)`
`dhcpagent`	Setzt Parameterwerte für den `dhcpagent`-Client-Daemon. Der Pfad zur Datei lautet `/etc/default/dhcpagent`. Informationen zu den Parametern finden Sie in der Datei `/etc/default/dhcpagent` oder in der Manpage `dhcpagent(1M)`.	`dhcpagent(1M)`

TABELLE 18–2 Von DHCP-Daemons und -Befehlen verwendete Dateien und Tabellen *(Fortsetzung)*

Datei- oder Tabellenname	Beschreibung	Manpage
DHCP `inittab`	Definiert Aspekte der DHCP-Optionscodes, z. B. dem Datentyp, und weist Mnemonikbezeichnungen zu. Weitere Informationen zur Dateisyntax finden Sie in der Manpage `dhcp_inittab(4)`. Auf dem Client werden die Informationen in der Datei `/etc/dhcp/inittab` von `dhcpinfo` verwendet, um aussagekräftige Informationen für Benutzer bereitzustellen. Auf dem DHCP-Serversystem wird diese Datei vom DHCP-Daemon und den Verwaltungstools verwendet, um DHCP-Optionsinformationen zu beziehen. Die Datei `/etc/dhcp/inittab` ersetzt die Datei `/etc/dhcp/dhcptags`, die in früheren Releases verwendet wurde. „DHCP-Optionsinformationen“ auf Seite 506 enthält weitere Informationen zu dieser Ersetzung.	`dhcp_inittab(4)`

DHCP-Optionsinformationen

In der Vergangenheit wurden DHCP-Optionsinformationen an verschiedenen Orten gespeichert, z. B. in der `dhcptab`-Tabelle des Servers, in der `dhcptags`-Datei des Clients sowie in internen Tabellen verschiedener Programme. Ab Solaris 8 und aktuelleren Releases sind in die Optionsinformationen in der Datei `/etc/dhcp/inittab` zusammengefasst. Ausführliche Informationen zu dieser Datei finden Sie in der Manpage `dhcp_inittab(4)`.

Der Oracle Solaris DHCP-Client verwendet die DHCP `inittab`-Datei als Ersatz für die `dhcptags`-Datei. Der Client nutzt die Datei, um Informationen zu Optionscodes zu beziehen, die in einem DHCP-Paket empfangen wurden. Auch die Programme `in.dhcpd`, `snoop` und `dhcpmgr` auf dem DHCP-Server verwenden die Datei `inittab`.

Feststellen, ob Ihr Standort betroffen ist

Die meisten Standorte, die Oracle Solaris DHCP verwenden, sind von dem Wechsel zur */etc/dhcp/inittab*-Datei `nicht` betroffen. Ihr Standort ist nur dann betroffen, wenn alle folgenden Kriterien erfüllt sind:

- Sie beabsichtigen, von einer Oracle Solaris-Version vor Solaris 8 zu aktualisieren.
- Sie haben zuvor neue DHCP-Optionen erstellt.
- Sie haben Änderungen an der Datei `/etc/dhcp/dhcptags` vorgenommen, und Sie möchten diese Änderungen beibehalten.

Wenn Sie aktualisieren, werden Sie vom Aktualisierungsprotokoll benachrichtigt, dass Ihre `dhcptags`-Datei geändert wurde, und dass Sie diese Änderungen an der DHCP `inittab` vornehmen sollten.

Unterschiede zwischen den Dateien `dhcptags` und `inittab`

Die Datei `inittab` enthält mehr Informationen als die Datei `dhcptags.` Darüber hinaus verwendet die Datei `inittab` eine andere Syntax.

Ein Beispieleintrag in der Datei `dhcptags` ist:

```
33 StaticRt - IPList Static_Routes
```

`33` ist der numerische Code, der in dem DHCP-Paket übergeben wird. `StaticRt` ist der Optionsname. `IPList` kennzeichnet, dass der Datentyp für `StaticRt` eine Liste mit IP-Adressen sein muss. `Static_Routes` ist ein beschreibender Name.

Die Datei `inittab` besteht aus einzeiligen Datensätzen, die jeweils eine Option beschreiben. Das Format ähnelt dem, mit dem Symbole in `dhcptab` definiert werden. In der folgenden Tabelle ist die Syntax der `inittab`-Datei beschrieben.

Option	Beschreibung
Optionsname	Der Name der Option. Der Optionsname muss innerhalb seiner Optionskategorie einmalig sein und darf nicht mit anderen Optionsnamen in den Kategorien „Standard“, „Standort“ und „Anbieter“ überlappen. So können Sie keine zwei „Standort“-Optionen mit dem gleichen Namen haben und sollten keine „Standort“-Option mit einem Namen erstellen, der schon für eine „Standard“-Option vergeben wurde.
Kategorie	Gibt den Namespace an, zu dem die Option gehört. Muss einer der Folgenden sein: „Standard“, „Standort“, „Anbieter“, „Feld“ oder „Intern“.
Code	Identifiziert die Option, wenn sie über das Netzwerk gesendet wird. In den meisten Fällen identifiziert der Code eine Option oder eine Kategorie einmalig. Bei den internen Kategorien wie „Feld“ oder „Intern“ kann ein Code jedoch auch für andere Zwecke verwendet werden. Der Code muss nicht global einmalig sein. Der Code sollte innerhalb der Optionskategorie einmalig sein und nicht mit Codes der Felder „Standard“ und „Standort“ überlappen.
type	Beschreibt die Daten, die mit dieser Option zugeordnet werden. Die gültigen Typen sind IP, ASCII, Oktett, Boolescher Wert, Unumber8, Unumber16, Unumber32, Unumber64, Snumber8, Snumber16, Snumber32 und Snumber64. Bei Zahlen gibt ein einleitendes U oder S an, ob die Zahl vorzeichenlos oder vorzeichenbehaftet ist. Die Zahlen am Ende geben an, wie viele Bit in der Zahl vorhanden sind. Beispielsweise ist Unumber8 eine vorzeichenlose 8-Bit-Zahl. Der Typ ist unabhängig von der Groß-/Kleinschreibung.
Granularität	Beschreibt, wie viele Dateneinheiten den Gesamtwert für diese Option ausmachen.

Maximum Gibt an, wie viele ganze Werte für diese Option erlaubt sind. 0 bedeutet unendlich.

Nutzer Beschreibt, welche Programme diese Informationen nutzen können. Die Nutzer werden mit `sdmi` eingerichtet. Dabei gilt:

`s` `snoop`

`d` `in.dhcpd`

`m` `dhcpmgr`

`i` `dhcpinfo`

Ein `inittab`-Beispieleintrag ist:

```
StaticRt - Standard, 33, IP, 2, 0, sdmi
```

Dieser Eintrag beschreibt eine Option namens `StaticRt`. Die Option befindet sich in der Standardkategorie und besitzt den Optionscode 33. Die erwarteten Daten stellen eine potenziell unendliche Anzahl am IP-Adressen dar, da der Typ `IP`, die Granularität `2` und das Maximum unendlich (`0`) ist. Die Nutzer dieser Option sind `sdmi`: `snoop`, `in.dhcpd`, `dhcpmgr` und `dhcpinfo`.

Umwandeln von `dhcptags`-Einträgen zu `inittab`-Einträgen

Wenn Sie in der Vergangenheit Einträge zu Ihrer Datei `dhcptags` hinzugefügt haben, müssen Sie die entsprechenden Einträge in die neue Datei `inittab` einfügen, wenn Sie die Ihrem Standort hinzugefügten Optionen weiterhin verwenden möchten. Das folgende Beispiel zeigt, wie ein `dhcptags`-Eintrag im `inittab`-Format ausgedrückt werden könnte.

Angenommen, Sie haben den folgenden `dhcptags`-Eintrag für ein Faxgerät hinzugefügt, das mit dem Netzwerk verbunden ist:

```
128 FaxMchn - IP Fax_Machine
```

Der Code `128` bedeutet, dass sich die Option in der „Standort“-Kategorie befindet. Der Optionsname lautet `FaxMchn`, und der Datentyp ist `IP`.

Der entsprechende `inittab`-Eintrag wäre:

```
FaxMchn SITE, 128, IP, 1, 1, sdmi
```

Die Granularität von 1 und das Maximum von 1 geben an, dass eine IP-Adresse für diese Option erwartet wird.

TEIL IV

IP-Sicherheit

In diesem Abschnitt werden Aspekte der Netzwerksicherheit beschrieben. Die Sicherheitsarchitektur für IP (IP Security Architecture, IPsec) schützt das Netzwerk auf der Paketebene. Der Internet-Schlüsselaustausch (Internet Key Exchange, IKE) verwaltet die Schlüssel für IPsec. Oracle Solaris IP Filter stellt eine Firewall bereit.

KAPITEL 19

IP Security Architecture (Übersicht)

Die IP Security Architecture (IPsec) bietet grafischen Schutz für IP-Datagramme in IPv4- und IPv6-Netzwerkpaketen.

Dieses Kapitel enthält die folgenden Informationen:

- „Neuerungen in IPsec" auf Seite 511
- „Einführung in IPsec" auf Seite 513
- „IPsec-Paketfluss" auf Seite 516
- „IPsec und Sicherheitszuordnungen" auf Seite 519
- „IPsec-Schutzmechanismen" auf Seite 520
- „IPsec-Schutzrichtlinien" auf Seite 524
- „Transport- und Tunnelmodi in IPsec" auf Seite 525
- „Virtuelle private Netzwerke und IPsec" auf Seite 527
- „IPsec und NAT Traversal" auf Seite 528
- „IPsec und SCTP" auf Seite 529
- „IPsec und Solaris Zones" auf Seite 529
- „IPsec und Logische Domains" auf Seite 530
- „IPsec-Dienstprogramme und Dateien" auf Seite 530
- „Änderungen an IPsec für Solaris 10 " auf Seite 532

Informationen zur Implementierung von IPsec in Ihrem Netzwerk finden Sie in Kapitel 20, „Konfiguration von IPsec (Aufgaben)". Referenzinformationen finden Sie in Kapitel 21, „IP Security Architecture (Referenz)".

Neuerungen in IPsec

Solaris 10 4/09: Ab dieser Version wird IPsec in der Service Management Facility (SMF) als Satz verschiedener Services verwaltet.

Standardmäßig werden beim Booten des Systems zwei IPsec-Services aktiviert:

- `svc:/network/ipsec/policy:default`
- `svc:/network/ipsec/ipsecalgs:default`

Standardmäßig sind die Schlüsselmanagement-Services beim Booten des Systems deaktiviert:

- `svc:/network/ipsec/manual-key:default`
- `svc:/network/ipsec/ike:default`

Gehen Sie wie folgt vor, um die IPsec-Richtlinien in SMF zu aktivieren:

1. Fügen Sie der Datei `ipsecinit.conf` IPsec-Richtlinieneinträge hinzu.
2. Konfigurieren Sie die Internet Key Exchange (IKE), oder konfigurieren Sie die Schlüssel manuell.
3. Aktualisieren Sie den Service für die IPsec-Richtlinie.
4. Aktivieren Sie den Schlüsselmanagement-Service.

Weitere Informationen zu SMF finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration*. Lesen Sie hierzu auch die Manpages `smf`(5) und `svcadm`(1M).

Ab dieser Version steht für die Befehle `ipsecconf` und `ipseckey` die Option `-c` zur Verfügung. Hiermit wird die Syntax der jeweiligen Konfigurationsdateien überprüft. Außerdem wird das neue Rechteprofil für das Netzwerk-IPsec-Management bereitgestellt. Dies wird zur Verwaltung von IPsec und IKE benötigt.

Solaris 10 7/07: Ab diesem Release implementiert IPsec vollständig Tunnel im Tunnelmodus. Die Dienstprogramme, die Tunnel unterstützen, wurden modifiziert.

- IPsec implementiert Tunnel im Tunnelmodus für virtuelle private Netzwerke (VPNs). Im Tunnelmodus unterstützt IPsec mehrere Clients hinter einem einzelnen NAT. Im Tunnelmodus kann IPsec mit Implementationen von IP-in-IP-Tunneln von anderen Anbietern zusammenarbeiten. IPsec unterstützt weiterhin Tunnel im Transportmodus, ist also mit früheren Solaris-Releases kompatibel.
- Die Syntax zum Erzeugen eines Tunnels wurde vereinfacht. Zur Verwaltung der IPsec-Richtlinie wurde der Befehl `ipsecconf` erweitert. Der Befehl `ifconfig` zur Verwaltung der IPsec-Richtlinie wird nicht unterstützt.
- Ab diesem Release ist die Datei `/etc/ipnodes` nicht mehr vorhanden. Verwenden Sie die Datei `/etc/hosts` zur Konfiguration der IPv6-Netzwerkschnittstellen.

Solaris 10 1/06: Ab diesem Release ist IKE vollständig konform mit NAT-Traversal-Unterstützung gemäß der Normen RFC 3947 und RFC 3948. IKE-Operationen nutzen die PKCS #11-Bibliothek des Solaris Cryptographic Framework (SCF), was die Leistung verbessert.

Das Kryptographie-Framework stellt einen Softtoken-Schlüsselspeicher für Anwendungen bereit, die den Metaslot verwenden. Wenn IKE den Metaslot verwendet, können Sie die Schlüssel auf einer Festplatte, einem angehängten Board oder im Softtoken-Schlüsselspeicher speichern.

- Informationen zur Verwendung des Softtoken-Schlüsselspeichers finden Sie in der Manpage `cryptoadm(1M)`.
- Eine vollständige Liste der neuen Funktionen in Solaris sowie eine Beschreibung der Solaris-Versionen finden Sie in *Neuerungen in Oracle Solaris 9 10/10*.

Einführung in IPsec

IPsec schützt IP-Pakete, indem es Pakete authentifiziert, Pakete verschlüsselt oder beides ausführt. IPsec wird innerhalb des IP-Moduls unterhalb der Anwendungsschicht ausgeführt. Aus diesem Grund kann eine Internet-Anwendung die Vorteile von IPsec nutzen, ohne dass sie zur Verwendung von IPsec konfiguriert werden muss. Wenn es richtig eingesetzt wird, ist IPsec ein wirksames Tool bei der Sicherung des Netzwerkverkehrs.

Der IPsec-Schutz umfasst fünf Hauptkomponenten:

- **Sicherheitsprotokolle –** Die Schutzmechanismen für IP-Datagramme. Der Authentication Header (AH) signiert IP-Pakete und stellt so Integrität sicher. Der Inhalt des Datagramms wird nicht verschlüsselt, aber der Empfänger kann sicher sein, dass der Paketinhalt nicht geändert wurde. Darüber hinaus wird dem Empfänger versichert, dass die Pakete vom Absender gesendet wurden. Die Encapsulating Security Payload (ESP) verschlüsselt IP-Daten und verbirgt so den Inhalt während der Paketübertragung. ESP kann darüber hinaus die Datenintegrität über eine Authentifizierungs-Algorithmusoption sicherstellen.
- **Sicherheitszuordnung-Datenbank (SADB) –** Die Datenbank, die ein Sicherheitsprotokoll mit einer IP-Zieladresse und eine Indexnummer verbindet. Die Indexnummer wird als Security Parameter Index (SPI) bezeichnet. Diese drei Elemente (das Sicherheitsprotokoll, die Zieladresse und die SPI) kennzeichnen ein legitimes IPsec-Paket eindeutig. Die Datenbank stellt sicher, dass ein geschütztes Paket, das am Ziel eintrifft, auch vom Empfänger erkannt wird. Der Empfänger verwendet die Informationen aus der Datenbank, um den Datenverkehr zu entschlüsseln, um sicherzustellen, dass die Pakete nicht geändert wurden, um die sie wieder zusammenzusetzen und an das endgültige Ziel weiterzuleiten.
- **Schlüsselmanagement –** Das Erzeugen und Verteilen der Schlüssel für die kryptografischen Algorithmen und für die SPI.
- **Sicherheitsmechanismen –** Die Authentifizierungs- und Verschlüsselungsalgorithmen, mit denen die Daten in den IP-Datagrammen geschützt werden.
- **Security Policy-Datenbank (SPD) –** Die Datenbank, in der die Schutzebene angegeben ist, die für ein bestimmtes Datenpaket gilt. Die SPD filtert IP-Datenverkehr und stellt auf diese Weise fest, wie die Pakete verarbeitet werden müssen. Ein Paket kann vergeworfen werden. Ein Paket kann unverschlüsselt weitergeleitet werden. Ein Paket kann mit IPsec geschützt

werden. Bei abgehenden Paketen stellen SPD und SADB fest, welche Schutzebene angewendet werden soll. Bei eingehenden Paketen hilft die SPD festzustellen, ob die Schutzebene des Pakets akzeptabel ist. Wurde das Paket durch IPsec geschützt, wird die SPD abgefragt, nachdem das Paket entschlüsselt und geprüft wurde.

Beim Einsatz von IPsec werden die Sicherheitsmechanismen auf IP-Datagramme angewendet, die zur IP-Zieladresse gesendet werden. Der Empfänger nutzt die Informationen in seiner SADB, um die Legitimität ankommender Pakete sicherzustellen und sie zu entschlüsseln. Anwendungen können IPsec aufrufen, um ebenfalls Sicherheitsmechanismen an IP-Datagrammen auf Socket-Ebene anzuwenden.

Beachten Sie, dass sich Sockets je nach Port unterschiedlich verhalten:

- Für einen einzelnen Socket geltende SAs setzen ihren entsprechenden Port-Eingang in der SPD außer Kraft.
- Darüber hinaus gilt, ist ein Socket an einen Port angeschlossen und wird die IPsec-Richtlinie wird erst später an diesem Port angewendet, so wird der Datenverkehr, der diesen Socket verwendet, nicht durch IPsec geschützt.

  Natürlich wird ein Socket, der auf einem Port geöffnet wird, *nachdem* die IPsec-Richtlinie an diesem Port angewendet wurde, durch IPsec geschützt.

IPsec RFCs

Die Internet Engineering Task Force (IETF) hat eine Reihe von Requests for Comment (RFCs) veröffentlichen, in denen die Sicherheitsarchitektur für die IP-Schicht beschrieben wird. Das Copyright für diese RFCs liegt bei der Internet Society. Einen Link zu den RFCs finden Sie unter `http://www.ietf.org/`. Die folgende Liste der RFCs deckt die allgemeinen IP-Sicherheitsreferenzen ab:

- RFC 2411, „IP Security Document Roadmap,“ November 1998
- RFC 2401, „Security Architecture for the Internet Protocol,“ November 1998
- RFC 2402, „IP Authentication Header,“ November 1998
- RFC 2406, „IP Encapsulating Security Payload (ESP),“ November 1998
- RFC 2408, „Internet Security Association and Key Management Protocol (ISAKMP),“ November 1998
- RFC 2407, „The Internet IP Security Domain of Interpretation for ISAKMP,“ November 1998
- RFC 2409, „The Internet Key Exchange (IKE),“ November 1998
- RFC 3554, „On the Use of Stream Control Transmission Protocol (SCTP) with IPsec,“ Juli 2003 [in der Solaris 10-Release nicht implementiert]

IPsec-Terminologie

Die IPsec RFCs definieren zahlreiche Begriffe, mit denen Sie vertraut sein sollten, wenn Sie IPsec auf Ihren Systemen umsetzen möchten. In der folgenden Tabelle sind IPsec-Begriffe, ihre am häufigsten verwendeten Akronymen sowie Definitionen aufgeführt. Eine Liste der bei der Schlüsselaushandlung verwendeten Terminologie finden Sie in Tabelle 22–1.

TABELLE 19–1 IPsec-Begriffe, Akronymen und Definitionen

IPsec-Begriff	Acronym	Definition
Sicherheitszuordnung	SA	Eine einmalige Verbindung zwischen zwei Knoten in einem Netzwerk. Die Verbindung wird durch ein Triplet definiert: ein Sicherheitsprotokoll, ein Sicherheits-Parameterindex und ein ID-Ziel. Das IP-Ziel kann eine IP-Adresse oder ein Socket sein.
Sicherheitszuordnung-Datenbank	SADB	Eine Datenbank, in der alle aktiven Sicherheitszuordnungen enthalten sind.
Security Parameter Index	SPI	Der Indexwert für eine Sicherheitszuordnung. Ein SPI ist ein 32-Bit-Wert, der zwischen SAs unterscheidet, die das gleiche IP-Ziel und Sicherheitsprotokoll aufweisen.
Security Policy-Datenbank	SPD	Eine Datenbank, die feststellt, ob abgehende und eingehende Pakete die angegebene Schutzebene aufweisen.
Key Exchange		Der Prozess zum Erzeugen von Schlüsseln für asymmetrische kryptografische Algorithmen. Die zwei wichtigsten Methoden sind die RSA-Protokolle und das Diffie-Hellman-Protokoll.
Diffie-Hellman-Protokoll	DH	Ein Key Exchange-Protokoll zur Erzeugung und Authentifizierung von Schlüsseln. Wird häufig auch als *authentifizierter Schlüsselaustausch* bezeichnet.
RSA-Protokoll	RSA	Ein Key Exchange-Protokoll zur Erzeugung und Verteilung von Schlüsseln. Das Protokoll ist nach seinen drei Autoren Rivest, Shamir und Adleman benannt.
Internet-Sicherheitszuordnung und Schlüsselmanagement-protokoll	ISAKMP	Eine allgemeine Grundstruktur zum Einrichten des Formats für SA-Attribute sowie zum Aushandeln, Bearbeiten und Löschen von SAs. ISAKMP ist der IETF-Standard für die Verarbeitung von IPsec-SAs.

IPsec-Paketfluss

Abbildung 19–1 zeigt, wie ein IP-adressiertes Paket als Teil eines IP-Datagramms verarbeitet wird, wenn IPsec für ein abgehendes Paket aufgerufen wurde. Das Ablaufdiagramm zeigt, wo die Entitäten Authentication Header (AH) und Encapsulating Security Payload (ESP) am Paket angewendet werden können. Wie diese Entitäten angewendet werden und wie die Algorithmen ausgewählt werden, wird in den folgenden Abschnitten beschrieben.

Abbildung 19–2 zeigt den IPsec-Ablauf bei eingehenden Paketen.

ABBILDUNG 19–1 Ablauf bei IPsec für abgehende Pakete

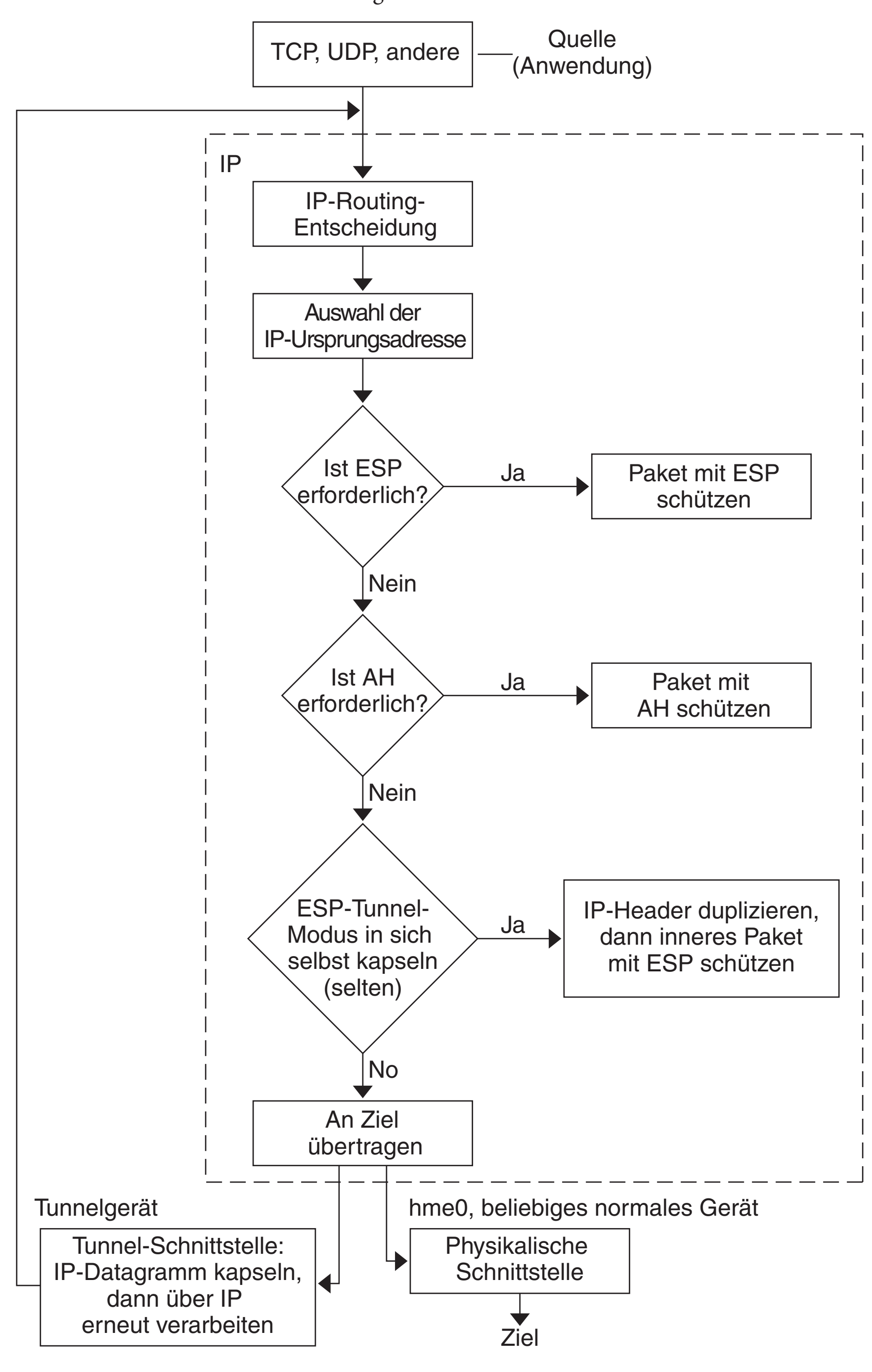
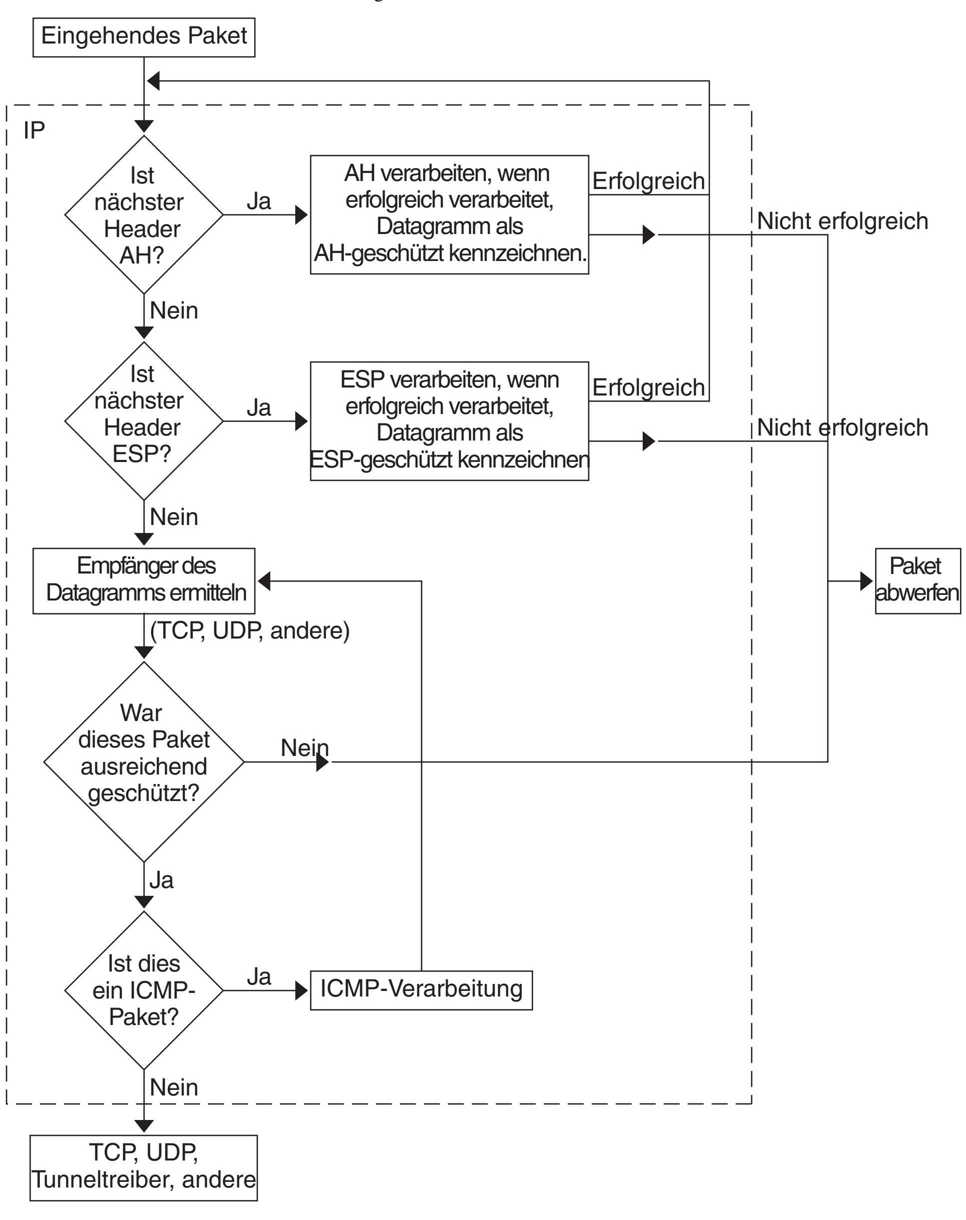


ABBILDUNG 19–2 Ablauf bei IPsec für eingehende Pakete



IPsec und Sicherheitszuordnungen

Eine IPsec-*Sicherheitszuordnung* (SA) legt die Sicherheitseigenschaften fest, die von miteinander kommunizierenden Hosts erkannt werden. Eine einzelne SA schützt Daten in eine Richtung. Der Schutz gilt entweder für einen bestimmten Host oder eine Gruppenadresse (multicast). Da eine Kommunikation entweder Peer-to-Peer oder Client-Server abläuft, müssen zwei SAs vorhanden sein, um den Datenverkehr in beide Richtungen zu schützen.

Eine IPsec-SA ist durch drei Elemente eindeutig gekennzeichnet:

- Das Sicherheitsprotokoll (AH oder ESP)
- Die IP-Zieladresse
- Den Security Parameter Index (SPI)

Der SPI, eine zufällige 32-Bit-Zahl, wird mit einem AH- oder ESP-Paket übertragen. In den Manpages `ipsecah(7P)` und `ipsecesp(7P)` finden Sie ausführliche Informationen zum Schutzumfang durch AH und ESP. Zur Authentifizierung eines Pakets wird eine Integrität-Prüfsumme eingesetzt. Schlägt die Authentifizierung fehl, wird das Paket verworfen.

Sicherheitszuordnungen werden in einer *Sicherheitszuordnung-Datenbank* (SADB) gespeichert. In berechtigten Anwendungen kann die Datenbank mithilfe einer Socket-basierten Verwaltungsengine, der `PF_KEY`-Schnittstelle, verwaltet werden. Beispielsweise können die IKE-Anwendung und der Befehl `ipseckeys` die Socketschnittstelle `PF_KEY` verwenden.

- Eine ausführliche Beschreibung der IPsec-SADB finden Sie unter „Sicherheitszuordnung-Datenbank für IPsec" auf Seite 597.
- Weitere Informationen zur Verwaltung der SADB finden Sie in der Manpage `pf_key(7P)`.

Schlüsselmanagement in IPsec

Sicherheitszuordnungen (SAs) benötigen Schlüsselmaterial zur Authentifizierung und Verschlüsselung. Die Verwaltung dieses *Schlüsselmaterials* wird als *Schlüsselmanagement* bezeichnet. Das Schlüsselmanagement wird automatisch vom Internet Key Exchange (IKE)-Protokoll abgewickelt. Sie können die Schlüssel jedoch auch manuell mit dem Befehl `ipseckey` verwalten.

SAs für IPv4- und IPv6-Pakete können beide Methoden zum Schlüsselmanagement verwenden. Solange kein zwingender Grund für ein manuelles Schlüsselmanagement vorliegt, sollten Sie das automatische Schlüsselmanagement einsetzen. Ein Grund für ein manuelles Schlüsselmanagement wäre die Zusammenarbeit mit Systemen, die nicht unter Solaris OS ausgeführt werden.

In der aktuellen Version stellt SMF IPsec die folgenden Schlüsselmanagement-Services bereit:

- `svc:/network/ipsec/ike:default` -**Service –** Der SMF-Service für das automatische Schlüsselmanagement. Der `ike`-Service führt zur Bereitstellung des automatischen Schlüsselmanagements den `in.iked`-Daemon aus. Eine Beschreibung des IKE-Protokolls finden Sie in Kapitel 22, „Internet Key Exchange (Übersicht)". Weitere Informationen zum `in.iked`-Daemon finden Sie in der Manpage `in.iked(1M)`. Informationen zum `ike`-Service finden Sie unter „IKE Service Management Facility" auf Seite 657.
- `svc:/network/ipsec/manual-key:default`-**Service –** Der SMF-Service für das manuelle Schlüsselmanagement. Der `manual-key`-Service führt den `ipseckey`-Befehl mit verschiedenen Optionen zum manuellen Schlüsselmanagement aus. Eine Beschreibung des `ipseckey` -Befehls finden Sie unter „Dienstprogramme zur Schlüsselerzeugung in IPsec" auf Seite 598. Eine ausführliche Beschreibung der `ipseckey`-Befehlsoptionen finden Sie in der Manpage `ipseckey(1M)`.

In älteren Versionen als Solaris 10 4/09 dienen die Befehle `in.iked` und `ipseckey` zur Verwaltung von Schlüsselmaterial.

- Der `in.iked`-Daemon bietet automatisches Schlüsselmanagement. Eine Beschreibung des IKE-Protokolls finden Sie in Kapitel 22, „Internet Key Exchange (Übersicht)". Weitere Informationen zum `in.iked`-Daemon finden Sie in der Manpage `in.iked(1M)`.
- Der `ipseckey`-Befehl bietet manuelles Schlüsselmanagement. Eine Beschreibung dieses Befehls finden Sie unter „Dienstprogramme zur Schlüsselerzeugung in IPsec" auf Seite 598. Eine ausführliche Beschreibung der `ipseckey`-Befehlsoptionen finden Sie in der Manpage `ipseckey(1M)`.

IPsec-Schutzmechanismen

IPsec umfasst zwei Sicherheitsprotokolle zum Schutz von Daten:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Ein AH schützt Daten mit einem Authentifizierungsalgorithmus. Eine ESP schützt Daten mit einem Verschlüsselungsalgorithmus. Optional kann eine ESP Daten mit einem Authentifizierungsalgorithmus schützen. Jede Implementierung eines Algorithmus wird als ein *Mechanismus* bezeichnet.

Authentication Header

Der Authentication Header bietet Datenauthentifizierung, starke Integrität und Replay-Schutz für IP-Datagrammen. AH schützt den größten Teil des IP-Datagramms. Wie die folgende Abbildung zeigt, wird der AH zwischen IP-Header und Transport-Header eingefügt.

IP-Hdr	AH	TCP-Hdr	

Der Transport-Header kann TCP, UDP, SCTP oder ICMP sein. Wenn ein Tunnel verwendet wird, kann der Transport-Header ein anderer IP-Header sein.

Encapsulating Security Payload

Das Encapsulating Security Payload (ESP)-Modul bietet Vertraulichkeit für Inhalte, die durch ESP eingekapselt sind. ESP stellt auch Services bereit, die vom AH angeboten werden. ESP stellt seinen Schutz jedoch nur dem Teil des Datagramms zur Verfügung, den ESP einkapselt. ESP bietet optionale Authentifizierungsservices, um die Integrität des geschützten Pakets sicherzustellen. Da ESP eine verschlüsselungskonforme Technologie verwendet, könnte ein System zur ESP-Bereitstellung den Gesetzen zu Exportbeschränkungen unterliegen.

ESP kapselt seine Daten ein, so dass ESP nur die Daten schützt, die seinem Anfang im Datagramm folgen, wie in der folgenden Abbildung gezeigt.

IP-Hdr	ESP	TCP-Hdr	

Verschlüsselt

In einem TCP-Paket kapselt ESP nur den TCP-Header und dessen Daten ein. Handelt es sich bei dem Paket um ein IP-in-IP-Datagramm, schützt ESP das innere IP-Datagramm. Die für einen Socket geltende Richtlinie ermöglicht eine *Selbst-Einkapselung*, so dass ESP gegebenenfalls auch IP-Optionen einkapseln kann.

Bei aktivierter Selbst-Einkapselung wird eine Kopie des IP-Headers erstellt, um ein IP-in-IP-Datagramm zu konstruieren. Ist die Selbst-Einkapselung nicht auf ein TCP-Socket gesetzt, wird das Datagramm in dem folgenden Format gesendet:

```
[ IP(a -> b) options + TCP + data ]
```

Ist die Selbst-Einkapselung auf ein TCP-Socket gesetzt, wird das Datagramm in dem folgenden Format gesendet:

```
[ IP(a -> b) + ESP [ IP(a -> b) options + TCP + data ] ]
```

Weitere Informationen finden Sie unter „Transport- und Tunnelmodi in IPsec“ auf Seite 525.

Sicherheitsbetrachtungen beim Verwenden von AH und ESP

In der folgenden Tabelle werden AH und ESP hinsichtlich des gebotenen Schutzes miteinander verglichen.

TABELLE 19–2 Von AH und ESP in IPsec gebotener Schutz

Protokoll	Einbezogenes Paket	Schutz	Gegenüber Angriffen
AH	Schützt das Paket vom IP-Header bis zum Transport-Header	Bietet starke Integrität, Datenauthentifizierung: ■ Stellt sicher, dass der Empfänger genau das empfängt, was der Absender gesendet hat. ■ Ist anfällig gegenüber Replay-Angriffen, wenn für einen AH kein Replay-Schutz aktiviert ist.<remark role="writer">	Wiedergabe, Ausschneiden und Einfügen
ESP	Schutz für das Paket ab dem Anfang der ESP im Datagramm.	Mit der Verschlüsselungsoption wird das IP-Datagramm verschlüsselt. Stellt Vertraulichkeit sicher.	Mithören
		Bietet mit der Authentifizierungsoption den gleichen Schutz wie der AH.	Wiedergabe, Ausschneiden und Einfügen
		Bietet mit beiden Optionen starke Integrität, Datenauthentifizierung und Vertraulichkeit.	Wiedergabe, Ausschneiden und Einfügen, Mithören

Authentifizierungs- und Verschlüsselungsalgorithmen in IPsec

Die IPsec-Sicherheitsprotokolle verwenden zwei Arten von Algorithmen: Authentifizierung und Verschlüsselung. Das AH-Modul verwendet Authentifizierungsalgorithmen. Das ESP-Modul kann sowohl Verschlüsselungs- als auch Authentifizierungsalgorithmen verwenden. Eine Liste der auf Ihrem System verwendeten Algorithmen und deren Eigenschaften können Sie durch Eingabe des Befehls `ipsecalgs` anzeigen. Weitere Informationen finden Sie in der Manpage `ipsecalgs(1M)` Mit den in der Manpage `getipsecalgbyname(3NSL)` beschriebenen Funktionen können Sie auch die Eigenschaften der Algorithmen abrufen.

IPsec auf einem Solaris-System verwendet die kryptografische Grundstruktur in Solaris, um auf die Algorithmen zuzugreifen. Die Grundstruktur bietet neben anderen Services auch ein zentrales Repository für Algorithmen. Mithilfe der Grundstruktur kann IPsec von den leistungsstarken kryptografischen Hardwarebeschleunigern profitieren. Darüber hinaus stellt die Grundstruktur Resource Control-Funktionen zur Verfügung. Beispielsweise können Sie mit der Grundstruktur die Zeit beschränken, die die CPU für kryptografischen Vorgänge im Kernel aufwendet.

Weitere Informationen finden Sie hier:

- Kapitel 13, „Oracle Solaris Cryptographic Framework (Overview)" in *System Administration Guide: Security Services*
- Kapitel 8, „Introduction to the Oracle Solaris Cryptographic Framework" in *Oracle Solaris Security for Developers Guide*

Authentifizierungsalgorithmen in IPsec

Authentifizierungsalgorithmen erzeugen eine Integritätsprüfsumme (*digest*), die auf den Daten und einem Schlüssel basiert. Das AH-Modul verwendet Authentifizierungsalgorithmen. Das ESP-Modul kann ebenfalls Authentifizierungsalgorithmen verwenden.

Verschlüsselungsalgorithmen in IPsec

Verschlüsselungsalgorithmen verschlüsseln Daten mithilfe eines Schlüssels. Das ESP-Modul in IPsec verwendet Verschlüsselungsalgorithmen. Der Algorithmus arbeitet mit Daten in Einheiten von jeweils einer *Blockgröße*.

Verschiedene Versionen des Betriebssystems Solaris 10 enthalten verschiedenene Standard-Verschlüsselungsalgorithmen.

Achtung – Ab Solaris 10 7/07 brauchen Sie das Solaris Encryption Kit auf Ihrem System nicht zusätzlich zu installieren. Das Kit stuft den Patch-Level zur Verschlüsselung auf Ihrem System herab. Das Kit ist mit der Verschlüsselung auf Ihrem System nicht kompatibel.

- Ab Release Solaris 10 7/07 wird der Inhalt des Solaris Encryption Kit vom Solaris-Installationsdatenträger installiert. Bei dieser Version sind die SHA2-Authentifizierungsalgorithmen sha256, sha384 und sha512 hinzugefügt. Die SHA2-Implementierungen entsprechen der Spezifikation RFC 4868. Bei dieser Version werden größere Diffie-Hellman-Gruppen hinzugefügt: 2048-Bit (Gruppe 14), 3072-Bit (Gruppe 15) und 4096-Bit (Gruppe 16). Bei Sun-Systemen mit CoolThreads-Technologie wird nur die 2048-Bit-Gruppe beschleunigt.
- Vor Release Solaris 10 7/07 enthielt der Solaris-Installationsdatenträger grundlegende Algorithmen und Sie konnten stärkere Algorithmen aus dem Solaris Encryption Kit installieren.

  Standardmäßig sind die Algorithmen DES-CBC, 3DES-CBC, AES-CBC und Blowfish-CBC installiert. Die von den AES-CBC- und Blowfish-CBC-Algorithmen unterstützte Schlüsselgröße beträgt 128 Bit.

  AES-CBC- und Blowfish-CBC-Algorithmen, die Schlüsselgrößen von mehr als 128 Bit unterstützen, stehen IPsec zur Verfügung, wenn Sie das Solaris Encryption Kit installieren. Jedoch stehen nicht alle Verschlüsselungsalgorithmen auch außerhalb der Vereinigten Staaten von Amerika zur Verfügung. Das Kit ist als eine separate CD erhältlich, die *nicht* im Solaris 10-Installationspaket enthalten ist. Die Installation des Kit ist im *Solaris 10*

Encryption Kit Installation Guide beschrieben. Weitere Informationen finden Sie auf der Sun Downloads-Website (http://www.oracle.com/technetwork/indexes/downloads/index.html). Zum Herunterladen des Kits klicken Sie auf die Registerkarte „Downloads A-Z" und dann auf den Buchstaben S. Das Solaris 10 Encryption Kit befindet sich unter den 20 ersten Einträgen.

IPsec-Schutzrichtlinien

IPsec-Schutzrichtlinien können für alle Sicherheitsmechanismen verwendet werden. IPsec-Richtlinien können auf folgenden Ebenen angewendet werden:

- Auf systemweite Ebene
- Auf für einen Socket geltenden Ebene

IPsec wendet die systemweit geltende Richtlinie an abgehenden und eingehenden Datagrammen an. Abgehende Datagramme werden entweder geschützt oder ungeschützt gesendet. Bei aktiviertem Schutz sind die Algorithmen entweder spezifisch oder nicht spezifisch. Aufgrund zusätzlicher Daten, die dem System bekannt sind, können Sie einige zusätzliche Regeln für abgehende Datagramme anwenden. Eingehende Datagramme werden entweder akzeptiert oder verworfen. Die Entscheidung, ob ein eingehendes Datagramm verworfen oder akzeptiert wird, basiert auf verschiedenen Kriterien, die manchmal überlappen oder widersprüchlich sind. Widersprüche werden gelöst, in dem festgelegt wird, welche Regel zuerst ausgewertet wird. Datenverkehr wird automatisch akzeptiert, es sei denn, ein Richtlinieneintrag gibt an, dass Datenverkehr alle weiteren Richtlinien umgehen soll.

Eine Richtlinie, die ein Datagramm normalerweise schützt, kann umgangen werden. Sie können eine Ausnahme entweder in der systemweit geltenden Richtlinie angeben, oder Sie fordern an, das eine für ein Socket geltende Richtlinie umgegangen wird. Bei Datenverkehr innerhalb eines Systems werden Richtlinien erzwungen, aber tatsächliche Sicherheitsmechanismen nicht angewendet. Stattdessen wird die Richtlinie für abgehende Datenverkehr bei einem systeminternen Paket in ein eingehendes Paket übersetzt, für das die Mechanismen angewendet wurden.

Mit der Datei `ipsecinit.conf` und dem Befehl `ipsecconf` können Sie IPsec-Richtlinien konfigurieren. Einzelheiten und Beispiele finden Sie in der Manpage `ipsecconf`(1M).

Transport- und Tunnelmodi in IPsec

Die IPsec-Standards definieren zwei unterschiedlichen Modi für den IPsec-Betrieb: den *Transportmodus* und den *Tunnelmodus*. Die Modi wirken sich nicht auf die Verschlüsselung von Paketen aus. Die Pakete werden in beiden Modi durch AH, ESP oder durch beides geschützt. Die Modi unterscheiden sich in der Richtlinienauslegung, wenn es sich bei dem inneren Paket um ein ID-Paket handelt:

- Im Transportmodus bestimmt der äußere Header die IPsec-Richtlinie, die das innere IP-Paket schützt.
- Im Tunnelmodus bestimmt das innere IP-Paket die IPsec-Richtlinie, die dessen Inhalte schützt.

Im Transportmodus können der äußere Header, der nächste Header und alle Ports, die der nächste Header unterstützt, zum Festlegen der IPsec-Richtlinie verwendet werden. Somit kann IPsec aufgrund der Granularität eines einzelnen Port unterschiedliche Transportmodus-Richtlinien für zwei IP-Adressen erzwingen. Ist beispielsweise der nächste Header ein TCP-Header, der Ports unterstützt, kann die IPsec-Richtlinie für einen TCP-Port der äußeren IP-Adresse eingerichtet werden. Entsprechend gilt: ist der nächste Header ein IP-Header, können der äußere Header und der innere IP-Header zum Festlegen der IPsec-Richtlinie verwendet werden.

Der Tunnelmodus arbeitet nur für IP-in-IP-Datagramme. Tunneling im Tunnelmodus eignet sich dann, wenn Mitarbeiter von zu Hause aus eine Verbindung mit einem Zentralcomputer herstellen. Im Tunnelmodus wird die IPsec-Richtlinie für die Inhalte des inneren IP-Datagramms durchgesetzt. Bei mehreren verschiedenen inneren IP-Adressen können unterschiedliche IPsec-Richtlinien durchgesetzt werden. Das heißt, die innere IP-Adresse, der nächste Header, und Ports, die der nächste Header unterstützt, können eine Richtlinie durchsetzen. Im Gegensatz zum Transportmodus kann der äußere IP-Header im Tunnelmodus die Richtlinie für das innere IP-Datagramm nicht vorschreiben.

Aus diesem Grund kann die IPsec-Richtlinie im Tunnelmodus für Teilnetze eines LAN hinter einem Router und für Ports dieser Teilnetze angegeben werden. Eine IPsec-Richtlinie kann auch für bestimmte IP-Adressen (Hosts) in diesem Teilnetzen angegeben werden. Den Ports dieser Hosts kann auch jeweils eine bestimmte IPsec-Richtlinie zugewiesen sein. Wird jedoch ein dynamisches Routing-Protokoll über einen Tunnel ausgeführt, verwenden Sie keine Teilnetz- oder Adressauswahl, da sich die Ansicht der Netzwerktopologie auf dem Peer-Netzwerk ändern könnte. Änderungen würden die statische IPsec-Richtlinie ungültig machen. Beispiele für Tunneling-Verfahren, die eine Konfiguration statischer Routen beinhalten, finden Sie unter „Schützen eines VPN mit IPsec“ auf Seite 554.

In Solaris OS kann der Tunnelmodus nur für eine IP-Tunneling-Netzwerkschnittstelle erzwungen werden. Mit dem `ipsecconf`-Befehl wird ein `Tunnel`-Schlüsselwort bereitgestellt, um eine IP-Tunneling-Netzwerkschnittstelle auszuwählen. Ist das Schlüsselwort `tunnel` in einer Regel vorhanden, gelten alle in dieser Regel angegebenen Selektoren für das innere Paket.

Im Transportmodus kann das Datagramm durch ESP, AH oder durch beides geschützt werden.

Die folgende Abbildung zeigt eine IP-Adresse mit einem ungeschützten TCP-Paket.

ABBILDUNG 19–3 Ungeschütztes IP-Paket mit TCP-Informationen

IP-Hdr	TCP-Hdr	

Im Transportmodus schützt ESP die Daten wie in der folgenden Abbildung gezeigt. Der schattierte Bereich kennzeichnet den verschlüsselten Teil des Pakets.

ABBILDUNG 19–4 Geschütztes IP-Paket mit TCP-Informationen

IP-Hdr	ESP	TCP-Hdr	

Verschlüsselt

Im Transportmodus schützt AH die Daten wie in der folgenden Abbildung gezeigt.

ABBILDUNG 19–5 Von einem Authentication Header geschütztes Paket

IP-Hdr	AH	TCP-Hdr	

Tatsächlich schützt AH die Daten, bevor die Daten im Datagramm erscheinen. Entsprechend wirkt sich der Schutz durch den AH auch im Transportmodus auf einen Teil des IP-Headers aus.

Im Tunnelmodus befindet sich das gesamte Datagramm *innerhalb* des Schutzes eines IPsec-Headers. Das Datagramm in Abbildung 19–3 wird im Tunnelmodus durch einen äußeren IPsec-Header (in diesem Fall ESP) geschützt. Dies wird in der folgenden Abbildung gezeigt.

ABBILDUNG 19–6 Im Tunnelmodus geschütztes IPsec-Paket

IP-Hdr	ESP	IP-Hdr	TCP-Hdr

Verschlüsselt

Der Befehl `ipsecconf` umfasst Schlüsselwörter zum Einrichten von Tunneln im Tunnel- oder Transportmodus.

- Einzelheiten zur für einen Socket geltenden Richtlinie finden Sie in der Manpage `ipsec(7P)`.
- Ein Beispiel einer für einen Socket geltenden Richtlinie finden Sie unter „How to Use IPsec to Protect a Web Server From Nonweb Traffic“ auf Seite 539.
- Weitere Informationen zu Tunneln finden Sie in der Manpage `ipsecconf(1M)`.
- Ein Beispiel für eine Tunnelkonfiguration finden Sie unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560.

Virtuelle private Netzwerke und IPsec

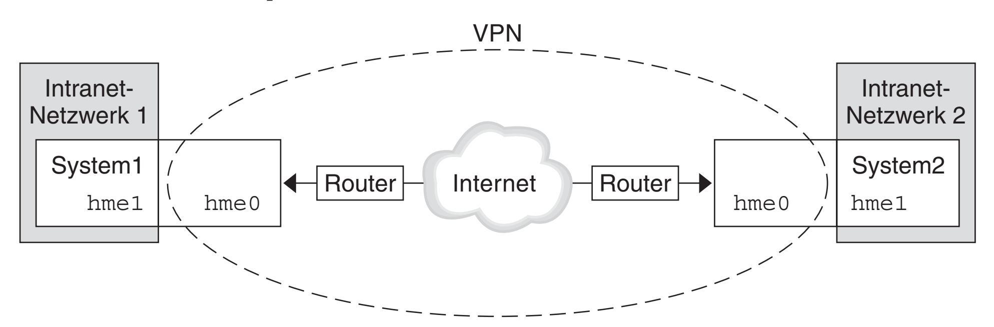
Ein konfigurierter Tunnel ist eine Point-to-Point-Schnittstelle. Ein Tunnel ermöglicht, dass ein IP-Paket in einem anderen IP-Paket eingekapselt wird. Ein korrekt konfigurierter Tunnel erfordert sowohl eine Tunnelquelle als auch ein Tunnelziel. Weitere Informationen finden Sie in der Manpage `tun(7M)` und unter Konfiguration von Tunneln zur Unterstützung von IPv6.

Ein Tunnel erstellt eine scheinbare Physikalische Schnittstelle für IP. Die Integrität einer physikalischen Verknüpfung hängt von den zu Grunde liegenden Sicherheitsprotokollen ab. Wenn Sie die Sicherheitszuordnungen (SAs) sicher einrichten, können Sie dem Tunnel vertrauen. Pakete, die den Tunnel verlassen, müssen von dem Peer stammen, der am Tunnelziel angegeben wurde. Wenn diese Vertrauensstellung existiert, können Sie eine für eine Schnittstelle geltende IP-Weiterleitung verwenden, um ein Virtuelles privates Netzwerk (VPN) zu erstellen.

Ein VPN kann mithilfe von IPsec erstellt werden. IPsec sichert die Verbindung. So kann eine Organisation, die zwei Büros mit separaten Netzwerken über ein VPN verbindet, IPsec zur Sicherung des Datenverkehrs zwischen den zwei Büros verwenden.

Die folgende Abbildung zeigt, wie zwei Büros das Internet verwenden, um deren VPN einzurichten, das IPsec in den Netzwerksystemen einsetzt.

ABBILDUNG 19–7 Virtuelles privates Netzwerk



Ein ausführliches Beispiel zur Einrichtung dieses Systems finden Sie unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560.

Ein ähnliches Beispiel mit IPv6-Adressen finden Sie unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv6“ auf Seite 570.

IPsec und NAT Traversal

IKE kann IPsec SAs über eine NAT-Box aushandeln. Mit dieser Fähigkeit sind Systeme in der Lage, von einem standortfernen Netzwerk aus auch dann eine sichere Verbindung herzustellen, wenn sich die Systeme hinter einem NAT-Gerät befinden. Beispiele können Mitarbeiter, die von zu Hause aus arbeiten, oder Personen, die sich von einer Konferenz-Site aus anmelden, ihren Datenverkehr mit IPsec schützen.

NAT bedeutet Network Address Translation (Netzwerk-Adresseübersetzung). Eine NAT-Box dient zum Übersetzen einer privaten internen Adresse in eine einmalige Internetadresse. NATs befinden sich häufig an öffentlichen Zugangspunkten zum Internet, z. B. in Hotels. Weitere Informationen finden Sie unter „Verwenden der NAT-Funktion in Oracle Solaris IP Filter“ auf Seite 674.

Die Fähigkeit, IKE verwenden zu können, wenn sich eine NAT-Box zwischen kommunizierenden Systemen befindet, wird NAT-Traversal oder NAT-T genannt. In Release Solaris 10 gelten für NAT-T die folgenden Einschränkungen:

- NAT-T arbeitet nur mit IPv4-Netzwerken.
- NAT-T kann die Vorteile der IPsec ESP-Beschleunigung durch das Sun Crypto Accelerator 4000-Board nicht nutzen. Dennoch funktioniert die IKE-Beschleunigung mit dem Sun Crypto Accelerator 4000-Board.
- Das AH-Protokoll beruht auf einem unveränderlichen IP-Header. Aus diesem Grund funktioniert AH nicht mit NAT-T. Mit NAT-T wird das ESP-Protokoll verwendet.
- Die NAT-Box benötigt keine speziellen Verarbeitungsregeln. Eine NAT-Box mit speziellen IPsec-Verarbeitungsregeln zu Problemen mit der Implementierung von NAT-T führen.

- NAT-T arbeitet nur dann, wenn der IKE-Initiator das System hinter der NAT-Box ist. Ein IKE-Antwortgeber kann sich nicht hinter einer NAT-Box befinden, es sei denn, die Box wurde zum Weiterleiten von IKE-Paketen zum entsprechenden individuellen System hinter der Box programmiert.

Die folgenden RFCs beschreiben die NAT-Funktionalität und die Einschränkungen von NAT-T. Diese RFCs können Sie von `http://www.rfc-editor.org` herunterladen.

- RFC 3022, „Traditional IP Network Address Translator (Traditional NAT),“ Januar 2001
- RFC 3715, „IPsec-Network Address Translation (NAT) Compatibility Requirements,“ März 2004
- RFC 3947, „Negotiation of NAT-Traversal in the IKE,“ Januar 2005
- RFC 3948, „UDP Encapsulation of IPsec Packets,“ Januar 2005

Informationen zum Verwenden von IPsec über ein NAT finden Sie unter „Konfiguration von IKE für mobile Systeme (Übersicht der Schritte)“ auf Seite 642.

IPsec und SCTP

Das Solaris-Betriebssystem unterstützt das SCTP-Protokoll (Streams Control Transmission Protocol). Die Verwendung des SCTP-Protokolls und der SCTP-Portnummer zur Angabe einer IPsec-Richtlinie wird unterstützt, ist aber nicht sehr robust. Die IPsec-Erweiterungen für SCTP gemäß der Angabe in der RFC 3554 wurden noch nicht implementiert. Diese Einschränkungen können zu Komplikationen beim Erstellen einer IPsec-Richtlinie für SCTP führen.

SCTP kann im Rahmen einer einzelnen SCTP-Assoziation mehrere Quell- und Zieladressen verwenden. Wenn die IPsec-Richtlinie an einer Quell- oder an einer Zieladresse angewendet wird, könnte die Kommunikation fehlschlagen, wenn SCTP die Quell- oder Zieladresse dieser Assoziation wechselt. Die IPsec-Richtlinie erkennt nur die ursprüngliche Adresse. Informationen zum SCTP finden Sie in den RFCs und unter „SCTP-Protokoll“ auf Seite 42.

IPsec und Solaris Zones

Für gemeinsame IP-Zonen wird IPsec von der globalen Zone aus konfiguriert. Die Konfigurationsdatei einer IPsec-Richtlinie, `ipsecinit.conf`, existiert nur in der globalen Zone. Die Datei kann Einträge enthalten, die für nicht-globale Zonen gelten und Einträge, die für die globale Zone gelten.

Für exklusive IP-Zonen wird IPsec von der nicht-globalen Zone aus konfiguriert.

Informationen zur Verwendung von IPsec mit Zonen finden Sie unter „Schützen von Datenverkehr mit IPsec“ auf Seite 534. Informationen zu Zonen finden Sie in Kapitel 16, „Einführung in Solaris Zones“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

IPsec und Logische Domains

IPsec arbeitet mit logischen Domänen. Die logische Domäne muss eine Version des Betriebssystems Solaris ausführen, die IPsec enthält, so zum Beispiel Solaris 10.

Um logische Domänen zu erstellen, müssen Sie Oracle VM Server für SPARC verwenden, der früher mit dem Begriff Logical Domains bezeichnet wurde. Informationen zur Konfiguration von logischen Domänen finden Sie in *Logical Domains 1.2 Administration Guide* oder *Oracle VM Server for SPARC 2.0 Administration Guide*.

IPsec-Dienstprogramme und Dateien

Aus Tabelle 19–3 geht hervor, welche Dateien, Befehle und Servicebezeichnungen zur Konfiguration und Verwaltung von IPsec verwendet werden. Der Vollständigkeit halber enthält die Tabelle die Dateien und Befehle des Schlüsselmanagements.

Ab Solaris 10 4/09 erfolgt das IPsec-Management über SMF. Weitere Informationen zu Servicebezeichnungen finden Sie in Kapitel 18, „Managing Services (Overview)" in *System Administration Guide: Basic Administration*.

- Anweisungen zur Umsetzung von IPsec in Ihrem Netzwerk finden Sie unter „Schützen des Datenverkehrs mit IPsec (Übersicht der Schritte)" auf Seite 533.
- Details zu den Dienstprogrammen und Dateien von IPsec finden Sie in Kapitel 21, „IP Security Architecture (Referenz)".

TABELLE 19–3 Liste der ausgewählten IPsec-Dienstprogramme und -Dateien

IPsec-Dienstprogramm, -Datei oder -Service	Beschreibung	Manpage
`svc:/network/ipsec/ipsecalgs`	Der SMF-Service, der in der aktuellen Version die IPsec-Algorithmen verwaltet.	`smf(5)`, `ipsecalgs(1M)`
`svc:/network/ipsec/manual-key`	Der SMF-Service, der in der aktuellen Version die manuellen Sicherheitszuordnungen (SAs) verwaltet.	`smf(5)`, `ipseckey(1M)`
`svc:/network/ipsec/policy`	Der SMF-Service, der in der aktuellen Version die IPsec-Richtlinie verwaltet.	`smf(5)`, `ipsecconf(1M)`
`svc:/network/ipsec/ike`	Der SMF-Service, der in der aktuellen Version für das automatische Management von IPsec-SAs sorgt.	`smf(5)`, `in.iked(1M)`
`/etc/inet/ipsecinit.conf`-Datei	IPsec-Richtliniendatei. In älteren Versionen als Solaris 10 4/09 wird IPsec beim Booten aktiviert, falls diese Datei vorhanden ist. In der aktuellen Version verwendet der SMF `policy`-Service diese Datei zur Konfiguration der IPsec-Richtlinie beim Booten des Systems.	`ipsecconf(1M)`

TABELLE 19–3 Liste der ausgewählten IPsec-Dienstprogramme und -Dateien *(Fortsetzung)*

IPsec-Dienstprogramm, -Datei oder -Service	Beschreibung	Manpage
ipsecconf-Befehl	IPsec-Richtlinienbefehl. Nützlich zum Anzeigen und Ändern der aktuellen IPsec-Richtlinie sowie zum Testen. In früheren Versionen als Solaris 10 4/09 wird in den Boot-Skripten mit dem Befehl ipsecconf die Datei /etc/inet/ipsecinit.conf gelesen, und anschließend wird IPsec aktiviert. In der aktuellen Version wird ipsecconf vom SMF policy-Service zur Konfiguration der IPsec-Richtlinie beim Booten des Systems verwendet.	ipsecconf(1M)
PF_KEY-Socket-Schnittstelle	Schnittstelle der Sicherheitszuordnung-Datenbank (SADB). Wickelt das manuelle und das automatische Schlüsselmanagement ab.	pf_key(7P)
ipseckey-Befehl	Der IPsec-Schlüsselbefehl für SAs. ipseckey ist ein Befehlszeilen-Frontend für die PF_KEY-Schnittstelle. ipseckey kann SAs erzeugen, abbrechen oder ändern.	ipseckey(1M)
/etc/inet/secret/ipseckeys-Datei	Schlüssel für IPsec SAs. In älteren Versionen als Solaris 10 4/09 wird, wenn die Datei ipsecinit.conf vorhanden ist, beim Booten des Systems automatisch die Datei ipseckeys gelesen. In der aktuellen Version wird ipseckeys vom SMF manual-key-Service zur manuellen Konfiguration von SAs beim Booten des Systems verwendet.	
ipsecalgs-Befehl	Befehl für IPsec-Algorithmen. Nützlich zum Anzeigen und Ändern der Liste von IPsec-Algorithmen und deren Eigenschaften. Wird in der aktuellen Version vom SMF ipsecalgs-Service beim Booten des Systems zur Synchronisierung bekannter IPsec-Algorithmen mit dem Systemkern verwendet.	ipsecalgs(1M)
/etc/inet/ipsecalgs-Datei	Enthält die konfigurierten IPsec-Protokolle und Definitionen der Algorithmen. Diese Datei wird vom ipsecalgs-Befehl verwaltet und darf nicht manuell bearbeitet werden.	
/etc/inet/ike/config-Datei	IKE-Konfigurations- und Richtliniendatei. Diese Datei ist standardmäßig nicht vorhanden. In älteren Versionen als Solaris 10 4/09 stellt der IKE-Daemon (in.iked) das automatische Schlüsselmanagement bereit, wenn diese Datei vorhanden ist. Das Management basiert auf Regeln und globalen Parametern in der Datei /etc/inet/ike/config. Lesen Sie dazu „IKE-Dienstprogramme und Dateien" auf Seite 608. In der aktuellen Version startet der svc:/network/ipsec/ike -Service den IKE-Daemon (in.iked) für das automatische Schlüsselmanagement, falls diese Datei vorhanden ist.	ike.config(4)

Änderungen an IPsec für Solaris 10

Eine vollständige Liste der neuen Funktionen in Solaris sowie eine Beschreibung der Solaris-Versionen finden Sie in *Neuerungen in Oracle Solaris 9 10/10*. Mit Solaris 9 wurden die folgenden Funktionen in IPsec eingeführt:

- Wenn ein Sun Crypto Accelerator 4000-Board angehängt ist, speichert das Board IPsec SAs für Pakete, die die Ethernet-Schnittstelle des Boards verwenden, automatisch im Cache-Speicher zwischen. Darüber hinaus beschleunigt das Board die Verarbeitung der IPsec SAs.
- IPsec profitiert von den Vorteilen des automatischen Schlüsselmanagements mit IKE über IPv6-Netzwerke. Weitere Informationen finden Sie in Kapitel 22, „Internet Key Exchange (Übersicht)“.

  Informationen zu den neuen IKE-Funktionen finden Sie unter „Änderungen an IKE für das Release Solaris 10“ auf Seite 610.
- Der Parser für den `ipseckey`-Befehl enthält eine besser strukturierte Hilfe. Der Befehl `ipseckey monitor` versieht jedes Ereignis mit einer Zeitmarke. Einzelheiten entnehmen Sie der Manpage `ipseckey(1M)`.
- IPsec-Algorithmen stammen jetzt aus einem zentralen Speicher, dem Solaris Cryptographic Framework. Eigenschaften der verfügbaren Algorithmen sind in der Manpage `ipsecalgs(1M)` beschrieben. Die Algorithmen sind für die Architektur optimiert, auf der sie ausgeführt werden. Eine Beschreibung des Framework finden Sie in Kapitel 13, „Oracle Solaris Cryptographic Framework (Overview)“ in *System Administration Guide: Security Services*.
- IPsec arbeitet in der globalen Zone. Die IPsec-Richtlinie wird in der globalen Zone für eine nicht-globale Zone verwaltet. Das Schlüsselmaterial wird manuell in der globalen Zone für eine nicht-globale Zone erzeugt und verwaltet. IKE kann nicht zum Erzeugen von Schlüsseln für eine nicht-globale Zonen verwendet werden. Weitere Informationen zu Zonen finden Sie in Kapitel 16, „Einführung in Solaris Zones“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.
- Die IPsec-Richtlinie kann mit dem Streams Control Transmission-Protokoll (SCTP) und der SCTP-Portnummer zusammenarbeiten. Dies wurde jedoch noch nicht vollständig realisiert. Die IPsec-Erweiterungen für SCTP, die in der RFC 3554 beschrieben sind, wurden an noch nicht umgesetzt. Diese Einschränkungen können zu Komplikationen beim Erstellen einer IPsec-Richtlinie für SCTP führen. Details finden Sie in den RFCs. Lesen Sie auch „IPsec und SCTP“ auf Seite 529 und „SCTP-Protokoll“ auf Seite 42.
- IPsec und IKE können Datenverkehr schützen, dessen Ursprung hinter einer NAT-Box liegt. Details und Einschränkungen finden Sie unter „IPsec und NAT Traversal“ auf Seite 528. Anweisungen finden Sie unter „Konfiguration von IKE für mobile Systeme (Übersicht der Schritte)“ auf Seite 642.

Konfiguration von IPsec (Aufgaben)

In diesem Kapitel sind die Verfahren zur Realisierung von IPsec in Ihrem Netzwerk beschrieben. Die Verfahren sind in den folgenden Tabellen beschrieben:

- „Schützen des Datenverkehrs mit IPsec (Übersicht der Schritte)" auf Seite 533
- „Schützen eines VPN mit IPsec (Übersicht der Schritte) " auf Seite 557

Eine Einführung in IPsec finden Sie in Kapitel 19, „IP Security Architecture (Übersicht)". Referenzinformationen zu IPsec finden Sie in Kapitel 21, „IP Security Architecture (Referenz)".

Schützen des Datenverkehrs mit IPsec (Übersicht der Schritte)

Die folgende Tabelle enthält Links zu den Verfahren, mit denen IPsec zwischen einem oder mehreren Systemen eingerichtet wird. Die Manpages `ipsecconf`(1M), `ipseckey`(1M) und `ifconfig`(1M) enthalten weitere nützliche Verfahren in den jeweiligen Beispiel-Abschnitten.

Aufgabe	Beschreibung	Siehe
Sichern des Datenverkehrs zwischen zwei Systemen.	Schützen Sie Pakete auf dem Weg von einem System zum anderen.	„So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec" auf Seite 535
Sichern eines Webbrowsers mithilfe einer IPsec-Richtlinie.	Erzwingen Sie, dass nicht-Webverkehr IPsec verwendet. Webclients werden durch die jeweiligen Ports identifiziert, die IPsec-Prüfungen umgehen.	„How to Use IPsec to Protect a Web Server From Nonweb Traffic" auf Seite 539
Anzeigen der IPsec-Richtlinien.	Zeigen Sie die derzeit durchgesetzten IPsec-Richtlinien in der Durchsetzungsreihenfolge an.	„So zeigen Sie die IPsec-Richtlinien an" auf Seite 542

Aufgabe	Beschreibung	Siehe
Erzeugen von Zufallszahlen.	Erzeugen Sie Zufallszahlen für das Schlüsselmaterial von manuell erstellten Sicherheitszuordnungen.	„So erzeugen Sie Zufallszahlen auf einem Solaris-System“ auf Seite 543 „How to Generate a Symmetric Key by Using the pktool Command“ in *System Administration Guide: Security Services*
Erstellen oder manuelles Ersetzen von Sicherheitszuordnungen.	Stellen Sie die Raw-Daten für Sicherheitszuordnungen bereit: ■ Name des IPsec-Algorithmus und Schlüsselmaterial ■ Schlüssel für den Security Parameter Index ■ IP-Quell- und Zieladressen	„So erstellen Sie manuell IPsec-Sicherheitszuordnungen“ auf Seite 545
Prüfen, ob IPsec die Pakete schützt.	Suchen Sie in der Ausgabe des Befehls `snoop` nach bestimmten Headern, die anzeigen, wie IP-Datagramme geschützt werden.	„So prüfen Sie, ob Pakete mit IPsec geschützt sind“ auf Seite 550
(Optional) Erstellen einer Network Security-Rolle.	Erstellen Sie eine Rolle, mit der ein sicheres Netzwerk eingerichtet werden kann, die aber über weniger Rechte als ein Superuser verfügt.	„How to Configure a Role for Network Security“ auf Seite 551
Verwalten von IPsec und Schlüsselmaterial als Gruppe von SMF-Services.	Beschreibt, wann und wie die Befehle zum Aktivieren, Deaktivieren, Aktualisieren und erneuten Starten von Services verwendet werden. Beschreibt außerdem die Befehle, die die Eigenschaftswerte von Services ändern.	„Verwalten von IKE- und IPsec-Services“ auf Seite 553
Einrichten eines sicheren virtuellen privaten Netzwerks (VPN).	Richten Sie IPsec zwischen zwei Systemen ein, die durch das Internet voneinander getrennt sind.	„Schützen eines VPN mit IPsec (Übersicht der Schritte) “ auf Seite 557

Schützen von Datenverkehr mit IPsec

Dieser Abschnitt enthält Verfahren, mit denen Sie den Datenverkehr zwischen zwei Systemen und einen Webserver sichern können. Informationen zum Schützen eines VPN finden Sie unter „Schützen eines VPN mit IPsec (Übersicht der Schritte) “ auf Seite 557. Zusätzliche Verfahren bieten Schlüsselmaterial und Sicherheitszuordnungen und stellen sicher, dass IPsec gemäß der Konfiguration arbeitet.

Die folgenden Informationen gelten für alle Aufgaben bei der Konfiguration von IPsec:

- **IPsec und Zonen –** Um die IPsec-Richtlinie und -Schlüssel für eine nicht-globale Zone mit gemeinsamer IP zu verwalten, erstellen Sie die IPsec-Richtliniendatei in der globalen Zone und führen die IPsec-Konfigurationsbefehle von der globalen Zone aus. Verwenden Sie die Quelladresse, die der von Ihnen konfigurierten nicht-globalen Zone entspricht. Sie können die IPsec-Richtlinie und -Schlüssel auch in der globalen Zone für die globale Zone konfigurieren. Für eine exklusive IP-Zone konfigurieren Sie die IPsec-Richtlinie in der nicht-globalen Zone. Ab Solaris 10 7/07 können Sie die Schlüssel in einer nicht-globalen Zone mit IKE verwalten.
- **IPsec und RBAC –** Informationen zum Verwenden von Rollen zur Verwaltung von IPsec finden Sie in Kapitel 9, „Using Role-Based Access Control (Tasks)" in *System Administration Guide: Security Services*. Ein Beispiel finden Sie unter „How to Configure a Role for Network Security" auf Seite 551.
- **IPsec und SCTP –** IPsec kann zum Schützen der Streams Control Transmission Protocol (SCTP)-Assoziationen verwendet werden, jedoch ist hier Vorsicht geboten. Weitere Informationen finden Sie unter „IPsec und SCTP" auf Seite 529.

▼ So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec

Dieses Verfahren nimmt das folgende Setup an:

- Die beiden Systeme heißen `enigma` und `partym`.
- Jedes System besitzt zwei Adressen, eine IPv4-Adresse und eine IPv6-Adresse.
- Jedes System erfordert eine ESP-Verschlüsselung mit dem AES-Algorithmus, was einen 128 Bit-Schlüssel erfordert, und ESP-Authentifizierung mit SHA1-Nachrichtendigest, was einen 160 Bit-Schlüssel erfordert.
- Jedes System verwendet gemeinsam genutzte Sicherheitszuordnungen.

  Bei gemeinsam genutzten SAs ist nur ein SA-Paar zum Schutz von zwei Systemen erforderlich.

Bevor Sie beginnen Sie müssen sich in der globalen Zone befinden, um die IPsec-Richtlinie für das System oder für eine gemeinsame IP-Zone zu konfigurieren. Für eine exklusive IP-Zone konfigurieren Sie die IPsec-Richtlinie in der nicht-globalen Zone.

1 Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

Hinweis – Eine Remoteanmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh` für eine sichere remote Anmeldung. Ein Beispiel finden Sie unter Beispiel 20–1.

---

2 Prüfen Sie auf jedem System Host-Einträge.

In der aktuellen Version fügen Sie die Hosteinträge der Datei `/etc/inet/hosts` hinzu.

Bei einem System, das ein älteres Release als Solaris 10 7/07 ausführt, fügen Sie die IPv4- und IPv6-Einträge zur Datei `/etc/inet/ipnodes` hinzu. Die Einträge für ein System müssen untereinander in der Datei stehen. „TCP/IP-Konfigurationsdateien" auf Seite 253Kapitel 11, „IPv6 im Detail (Referenz)".

Wenn Sie die Systeme nur mit IPv4-Adressen verbinden, nehmen Sie die Änderungen an der `/etc/inet/hosts`-Datei vor. In diesem Beispiel führen die zu verbindenden Systeme ein früheres Solaris-Release aus und verwenden IPv6-Adressen.

a. Geben Sie auf dem System `enigma` Folgendes in die Datei `hosts` bzw. `ipnodes` ein:

```
# Secure communication with partym
192.168.13.213 partym
2001::eeee:3333:3333 partym
```

b. Geben Sie auf dem System `partym` Folgendes in die Datei `hosts` bzw. `ipnodes` ein:

```
# Secure communication with enigma
192.168.116.16 enigma
2001::aaaa:6666:6666 enigma
```

Es ist unsicher, die Namensdienste für symbolische Namen zu verwenden.

3 Erstellen Sie auf jedem System die IPsec-Richtliniendatei.

Der Dateiname lautet `/etc/inet/ipsecinit.conf`. Ein Beispiel finden Sie in der Datei `/etc/inet/ipsecinit.sample`.

4 Fügen Sie einen IPsec-Richtlinieneintrag in die Datei `ipsecinit.conf` ein.

a. Fügen Sie die folgende Richtlinie auf dem System `enigma` hinzu:

```
{laddr enigma raddr partym} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. Fügen Sie eine identische Richtlinie auf dem System `partym` hinzu:

```
{laddr partym raddr enigma} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Informationen zur Syntax der IPsec-Richtlinieneinträge finden Sie in der Manpage `ipsecconf(1M)`.

5 Fügen Sie auf jedem System ein IPsec SA-Paar zwischen den zwei Systemen ein.

Sie können Internet Key Exchange (IKE) konfigurieren, um die SAs automatisch zu erstellen. Die SAs können auch manuell hinzugefügt werden.

Hinweis – Sie sollten IKE verwenden, es sei denn, Sie haben einen triftigen Grund, Ihre Schlüssel manuell zu erzeugen und zu verwalten. Das IKE-Schlüsselmanagement ist sicherer als das manuelle Schlüsselmanagement.

- Konfigurieren Sie IKE mithilfe eines der unter „Konfiguration von IKE (Übersicht der Schritte)“ auf Seite 611 beschriebenen Konfigurationsverfahren. Informationen zur Syntax der IKE-Konfigurationsdatei finden Sie in der Manpage `ike.config(4)`.
- Wie SAs manuell hinzugefügt werden, können Sie unter „So erstellen Sie manuell IPsec-Sicherheitszuordnungen“ auf Seite 545 nachlesen.

6 Aktivieren Sie die IPsec-Richtlinie.

- **Wenn Sie eine ältere Version als Solaris 10 4/09 verwenden, starten Sie das System neu.**

  ```
  # init 6
  ```

  Fahren Sie anschließend mit den Erläuterungen unter „So prüfen Sie, ob Pakete mit IPsec geschützt sind“ auf Seite 550 fort.

- **Aktualisieren Sie ab Solaris 10 4/09 den IPsec-Service, und aktivieren Sie den Schlüsselmanagement-Service.**

  Führen Sie Schritt 7 bis Schritt 10 durch.

7 Überprüfen Sie die Syntax der IPsec-Richtliniendatei.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

Beheben Sie alle Fehler, überprüfen Sie die Syntax der Datei, und fahren Sie fort.

8 Aktualisieren Sie die IPsec-Richtlinie.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

Die IPsec-Richtlinie wird standardmäßig aktiviert, daher sollten Sie sie *aktualisieren*. Falls Sie die IPsec-Richtlinie deaktiviert haben, aktivieren Sie sie.

```
# svcadm enable svc:/network/ipsec/policy:default
```

9 Aktivieren Sie die Schlüssel für IPsec.

- **Wenn Sie IKE in Schritt 5 konfiguriert haben, führen Sie eine der folgenden Aktionen durch:**

  - **Wenn der `ike`-Service nicht aktiviert ist, aktivieren Sie ihn.**

    ```
    # svcadm enable svc:/network/ipsec/ike:default
    ```

- **Wenn der `ike`-Service aktiviert ist, starten Sie ihn neu.**

```
# svcadm restart svc:/network/ipsec/ike:default
```

- **Wenn Sie in Schritt 5 Schlüssel manuell konfiguriert haben, führen Sie eine der folgenden Aktionen durch:**

  - **Wenn der `manual-key`-Service nicht aktiviert ist, aktivieren Sie ihn.**

  ```
  # svcadm enable svc:/network/ipsec/manual-key:default
  ```

  - **Wenn der `manual-key`-Service aktiviert ist, aktualisieren Sie ihn.**

  ```
  # svcadm refresh svc:/network/ipsec/manual-key:default
  ```

10 Prüfen Sie, ob die Pakete geschützt werden.

Informationen hierzu finden Sie unter „So prüfen Sie, ob Pakete mit IPsec geschützt sind" auf Seite 550.

Beispiel 20–1 Hinzufügen der IPsec-Richtlinie für eine `ssh`-Verbindung

In diesem Beispiel konfiguriert der Administrator als Superuser die IPsec-Richtlinie und die Schlüssel auf zwei Systemen mithilfe des Befehls `ssh`, um das zweite System zu erreichen. Weitere Informationen finden Sie in der Manpage `ssh`(1).

- Zunächst konfiguriert der Administrator das erste System durch Ausführen von Schritt 2 bis Schritt 5 des vorangegangenen Verfahrens.
- Dann verwendet der Administrator in einem anderen Terminal-Fenster den Befehl `ssh` zur Anmeldung am zweiten System.

```
local-system # ssh other-system
other-system #
```

- Im Terminal-Fenster der `ssh`-Sitzung konfiguriert der Administrator die IPsec-Richtlinie und die Schlüssel des zweiten Systems durch Ausführen von Schritt 2 bis Schritt 6.
- Dann beendet der Administrator die `ssh`-Sitzung.

```
other-system # exit
local-system #
```

- Schließlich aktiviert der Administrator die IPsec-Richtlinie auf dem ersten System durch Ausführen von Schritt 6.

Bei der nächsten Kommunikation der beiden Systeme, einschließlich einer `ssh`-Verbindung, wird die Kommunikation durch IPsec geschützt.

Beispiel 20–2 Schutz des Datenverkehrs mit IPsec ohne erneutes Booten

Das folgende Beispiel ist nützlich, wenn Sie mit einer älteren Version als Solaris 10 4/09 arbeiten. Zumindest, wenn in Ihrer Version IPsec nicht als Service verwaltet wird. Im Beispiel

wird beschrieben, wie Sie IPsec in einer Testumgebung implementieren. In einer Produktionsumgebung ist erneutes Booten des Systems sicherer als das Ausführen des Befehls `ipsecconf`. Informationen zu den Sicherheitsbetrachtungen finden Sie am Ende dieses Beispiels.

Anstatt in Schritt 6 neu zu booten, wählen Sie eine der folgenden Optionen:

- Wenn Sie IKE zum Erstellen des Schlüsselmaterials verwenden, müssen Sie den `in.iked`-Daemon zunächst stoppen und dann neu starten.

  ```
  # pkill in.iked
  # /usr/lib/inet/in.iked
  ```
- Wenn Sie die Schlüssel manuell hinzugefügt haben, verwenden Sie den Befehl `ipseckey`, um die SAs zur Datenbank hinzuzufügen.

  ```
  # ipseckey -c -f /etc/inet/secret/ipseckeys
  ```

  Dann aktivieren Sie die IPsec-Richtlinie mit dem Befehl `ipsecconf`.

  ```
  # ipsecconf -a /etc/inet/ipsecinit.conf
  ```

Sicherheitsbetrachtungen – Lesen Sie die Warnung, wenn Sie den Befehl `ipsecconf` ausführen. Ein bereits gesperrtes Socket, das heißt, ein Socket das bereits verwendet wird, stellt eine ungesicherte Hintertür zum System dar. For more extensive discussion, see „Sicherheitsbetrachtungen für `ipsecinit.conf` und `ipsecconf`“ auf Seite 596.

▼ How to Use IPsec to Protect a Web Server From Nonweb Traffic

Ein sicherer Webserver gestattet es Webclients, Daten untereinander über den Webservice auszutauschen. Auf einem sicheren Webserver *muss* Datenverkehr, bei dem es sich nicht um Webverkehr handelt, Sicherheitsprüfungen durchlaufen. Das folgende Verfahren beinhaltet Umgehungen für Webverkehr. Darüber hinaus kann dieser Webserver nicht sichere DNS-Client-Anforderungen stellen. Der gesamte verbleibende Verkehr erfordert ESP mit AES- und SHA-1-Algorithmen.

Bevor Sie beginnen Zur Konfiguration der IPsec-Richtlinie müssen Sie sich in der globalen Zone befinden. Für eine exklusive IP-Zone konfigurieren Sie die IPsec-Richtlinie in der nicht-globalen Zone. Sie haben den Abschnitt „So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec“ auf Seite 535 abgeschlossen, d. h. folgende Bedingungen sind wirksam:

- Die Kommunikation zwischen den beiden Systemen ist durch IPsec geschützt.
- Schlüsselmaterial wird manuell oder durch IKE generiert.
- Sie haben sichergestellt, dass Pakete geschützt werden.

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

   Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh` für eine sichere remote Anmeldung.

   ---

2. **Stellen Sie fest, welche Services Prüfungen der Sicherheitsrichtlinien umgehen müssen.**

   Bei einem Webserver umfassen diese Services TCP-Ports 80 (HTTP) und 443 (Secure HTTP). Wenn der Webserver DNS-Namenssuchen bereitstellt, muss der Server auch Port 53 für TCP und UDP umfassen.

3. **Erstellen Sie die IPsec-Richtlinie für den Webserver, und aktivieren Sie sie.**

   - **Befolgen Sie ab Solaris 10 4/09 Schritt 4 bis Schritt 7.**
   - **Wenn Sie mit einer älteren Version als Solaris 10 4/09 arbeiten, befolgen Sie die Schritte von Schritt 8 bis Schritt 11.**

   Schritt 12 ist in allen Solaris-Versionen optional.

4. **Fügen Sie der IPsec-Richtlinendatei die Webserver-Richtlinie hinzu.**

   Fügen Sie der Datei `/etc/inet/ipsecinit.conf` folgende Zeilen hinzu:

   ```
   # Web traffic that web server should bypass.
   {lport  80 ulp tcp dir both} bypass {}
   {lport 443 ulp tcp dir both} bypass {}

   # Outbound DNS lookups should also be bypassed.
   {rport 53 dir both} bypass {}

   # Require all other traffic to use ESP with AES and SHA-1.
   # Use a unique SA for outbound traffic from the port
   {} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
   ```

   Bei dieser Konfiguration ist nur bei sicherem Verkehr ein Zugriff auf das System möglich. Dabei gelten die in Schritt 4 beschriebenen Ausnahmen für die Umgehung.

5. **Überprüfen Sie die Syntax der IPsec-Richtliniendatei.**

   ```
   # ipsecconf -c -f /etc/inet/ipsecinit.conf
   ```

6 Aktualisieren Sie die IPsec-Richtlinie.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

7 Aktualisieren Sie die Schlüssel für IPsec.

- **Wenn Sie IKE in Schritt 5 von „So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec" auf Seite 535 konfiguriert haben, starten Sie den `ike`-Service neu.**

  ```
  # svcadm restart svc:/network/ipsec/ike
  ```

- **Wenn Sie Schlüssel in Schritt 5 von „So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec" auf Seite 535 manuell konfiguriert haben, starten Sie den `manual-key`-Service neu.**

  ```
  # svcadm refresh svc:/network/ipsec/manual-key:default
  ```

Ihre Einrichtung ist abgeschlossen. Sie können Schritt 12 optional durchführen.

8 Erstellen Sie eine Datei im Verzeichnis `/etc/inet` für die Webserver-Richtlinie.

Hinweis – Durch die folgenden Schritte wird ein Webserver konfiguriert, auf der eine ältere Version als Solaris 10 4/09 ausgeführt wird.

Benennen Sie die Datei mit einem aussagekräftigen Namen, z. B. `IPsecWebInitFile`. Geben Sie die folgenden Zeilen in diese Datei ein:

```
# Web traffic that web server should bypass.
{lport  80 ulp tcp dir both} bypass {}
{lport 443 ulp tcp dir both} bypass {}

# Outbound DNS lookups should also be bypassed.
{rport 53 dir both} bypass {}

# Require all other traffic to use ESP with AES and SHA-1.
# Use a unique SA for outbound traffic from the port
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Diese Konfiguration gestattet nur sicherem Verkehr den Zugriff auf das System. Dabei gelten die in Schritt 4 beschriebenen Ausnahmen für die Umgehung.

9 Kopieren Sie den Inhalt der von Ihnen in Schritt 8 erstellten Datei in die `/etc/inet/ipsecinit.conf`-Datei.

10 Schützen Sie die Datei `IPsecWebInitFile`, indem Sie Nur-Lese-Berechtigungen zuweisen.

```
# chmod 400 IPsecWebInitFile
```

11 Sichern Sie den Webserver, ohne ihn erneut zu booten.

Wählen Sie eine der folgenden Optionen:

- Wenn Sie IKE zum Schlüsselmanagement verwenden, stoppen Sie den `in.iked`-Daemon und starten ihn neu.

  ```
  # pkill in.iked
  # /usr/lib/inet/in.iked
  ```
- Wenn Sie die Schlüssel manuell verwalten, verwenden Sie die Befehle `ipseckey` und `ipsecconf`.

  Verwenden Sie `IPsecWebInitFile` als Argument für den Befehl `ipsecconf.` Wenn Sie die Datei `ipsecinit.conf` als Argument verwenden, erzeugt der Befehl `ipsecconf` Fehlermeldungen, wenn die Richtlinien in der Datei bereits auf dem System implementiert sind.

  ```
  # ipseckey -c -f /etc/inet/secret/ipseckeys
  # ipsecconf -a /etc/inet/IPsecWebInitFile
  ```

Achtung – Lesen Sie die Warnmeldung, wenn Sie den Befehl `ipsecconf` ausführen. Ein bereits gesperrtes Socket, das heißt, ein Socket das bereits verwendet wird, stellt eine ungesicherte Hintertür zum System dar. Ausführlichere Informationen finden Sie unter „Sicherheitsbetrachtungen für `ipsecinit.conf` und `ipsecconf`“ auf Seite 596. Die gleiche Warnmeldung gilt für den Neustart des `in.iked`-Daemon.

Sie können auch erneut booten. Durch erneutes Booten wird sichergestellt, dass die IPsec-Richtlinie für alle TCP-Verbindungen übernommen wird. Bei erneutem Booten verwenden die TCP-Verbindungen die Richtlinie in der IPsec-Richtliniendatei.

12 **(Optional) Konfigurieren Sie ein Remote-System so, dass es für NonWeb-Verkehr mit dem Webserver kommuniziert.**

Geben Sie die folgende Richtlinie die Datei `ipsecinit.conf` auf einem Remote-System ein:

```
# Communicate with web server about nonweb stuff
#
{laddr webserver} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Ein remotes System kann nur dann sicher mit dem Webserver NonWeb-Verkehr austauschen, wenn die IPsec-Richtlinien der Systeme übereinstimmen.

▼ So zeigen Sie die IPsec-Richtlinien an

Geben Sie den Befehl `ipsecconf` ohne weitere Argumente ein, um die auf dem System konfigurierten Richtlinien anzuzeigen.

Bevor Sie beginnen Sie müssen den Befehl `ipsecconf` in der globalen Zone ausführen. Führen Sie für eine exklusive IP-Zone den Befehl `ipsecconf` in der nicht-globalen Zone aus.

1 Nehmen Sie eine Rolle an, die das Network IPsec Management-Profil beinhaltet, oder melden Sie sich als Superuser an.

Wenn Sie eine ältere Version als Solaris 10 4/09 ausführen, ist das Profil für die Netzwerk-IPsec-Verwaltung nicht verfügbar. Verwenden Sie das Profil für Netzwerksicherheit.

Informationen zum Erstellen einer Rolle, die das Network Security-Profil beinhaltet und zum Zuweisen dieser Rolle zu einem Benutzer finden Sie unter „How to Configure a Role for Network Security“ auf Seite 551.

2 Anzeigen der IPsec-Richtlinien.

a. Zeigen Sie die Einträge in der globalen IPsec-Richtlinie in der Reihenfolge an, in der sie wurden.

```
$ ipsecconf
```

Mit diesem Befehl wird jedem Eintrag ein *Index* gefolgt von einer Zahl zugeordnet.

b. Zeigen Sie die Einträge der IPsec-Richtlinie in der Reihenfolge an, in der eine Übereinstimmung auftritt.

```
$ ipsecconf -l
```

c. Zeigen Sie die Einträge der IPsec-Richtlinie, einschließlich der für einen Tunnel geltenden Einträge, in der Reihenfolge an, in der eine Übereinstimmung auftritt.

```
$ ipsecconf -L
```

▼ So erzeugen Sie Zufallszahlen auf einem Solaris-System

Wenn Sie die Schlüssel manuell eingeben, muss das Schlüsselmaterial zufällig erzeugt worden sein. Bei einem Solaris-System muss das Schlüsselmaterial im hexadezimalen Format vorliegen. Andere Betriebssysteme erfordern Schlüsselmaterial im ASCII-Format. Informationen zum Erzeugen von Schlüsselmaterial für ein Solaris-System, das mit einem Betriebssystem kommuniziert, für das ASCII-Daten erforderlich sind, finden Sie in Beispiel 23–1.

Falls Ihr Standort über einen Generator für Zufallszahlen verfügt, verwenden Sie diesen. Andernfalls können Sie den Befehl `od` mit dem Solaris-Gerät `/dev/random` als Eingabe verwenden. Weitere Informationen finden Sie in der Manpage `od(1)`.

In der Solaris 10 4/09-Version können Sie auch den Befehl `pktool` verwenden. Die Syntax dieses Befehls ist einfacher als die Syntax des Befehls `od`. Weitere Informationen finden Sie unter „How to Generate a Symmetric Key by Using the pktool Command“ in *System Administration Guide: Security Services*

1 Erzeugen Sie hexadezimale Zufallszahlen.

% od -x|-X -A n *file* | head -*n*

`-x` Zeigt das oktale Abbild im hexadezimalen Format an. Das hexadezimale Format eignet sich für das Schlüsselmaterial. Der hexadezimale Wert wird in 4-Zeichen-Chunks gedruckt.

`-X` Zeigt das oktale Abbild im hexadezimalen Format an. Der hexadezimale Wert wird in 8-Zeichen-Chunks gedruckt.

`-A n` Löscht die Eingabe-Offsetbasis vom Bildschirm.

Datei Dient als Quelle für die Zufallszahlen.

`head -`*n* Beschränkt die Anzeige auf die ersten *n* Zeilen der Ausgabe.

2 Verbinden Sie die Ausgabe, um einen Schlüssel in der angegebenen Länge zu erzeugen.

Löschen Sie die Leerzeichen zwischen den Zahlen auf einer Zeile, um einen Schlüssel mit 32 Zeichen zu erzeugen. Ein 32-Zeichen-Schlüssel hat eine Länge von 128 Bit. Für den Security Parameter Index (SPI) sollten Sie einen 8-Zeichen-Schlüssel verwenden. Der Schlüssel sollte das Präfix `0x` verwenden.

Beispiel 20–3 Erzeugen des Schlüsselmaterials für IPsec

Im folgenden Beispiel werden zwei Zeilen mit Schlüsseln in Gruppen von jeweils acht hexadezimalen Zeichen angezeigt.

```
% od -X -A n /dev/random | head -2
         d54d1536 4a3e0352 0faf93bd 24fd6cad
         8ecc2670 f3447465 20db0b0c c83f5a4b
```

Durch Verbinden der vier Zeichengruppen in der ersten Zeile können Sie einen 32-Zeichen-Schlüssel erstellen. Eine 8-Zeichen-Zahl, die mit dem Präfix `0x` beginnt, ergibt einen geeigneten SPI-Wert, z. B. `0xf3447465`.

Im folgenden Beispiel werden zwei Zeilen mit Schlüsseln in Gruppen von jeweils vier hexadezimalen Zeichen angezeigt.

```
% od -x -A n /dev/random | head -2
         34ce 56b2 8b1b 3677 9231 42e9 80b0 c673
         2f74 2817 8026 df68 12f4 905a db3d ef27
```

Durch Verbinden der acht Zeichengruppen in der ersten Zeile können Sie einen 32-Zeichen-Schlüssel erstellen.

▼ So erstellen Sie manuell IPsec-Sicherheitszuordnungen

Im folgenden Verfahren wird das Schlüsselmaterial für das Verfahren „So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec“ auf Seite 535 erstellt. Sie generieren Schlüssel für die beiden Systeme `partym` und `enigma`. Sie generieren die Schlüssel auf einem System und verwenden dann die Schlüssel des ersten Systems auf beiden Systemen.

Bevor Sie beginnen Sie müssen sich in der globalen Zone befinden, um das Schlüsselmaterial für eine Zone mit gemeinsamer IP manuell verwalten zu können.

1. **Erzeugen Sie das Schlüsselmaterial für die SAs.**

   Sie benötigen drei hexadezimale Zufallszahlen für den abgehenden Verkehr und drei hexadezimale Zufallszahlen für den eingehenden Verkehr.

   Somit muss ein System die folgenden Zahlen erzeugen:

   - Zwei hexadezimale Zufallszahlen als Wert für das Schlüsselwort `spi.` Eine Zahl für den abgehenden Verkehr, eine Zahl für den eingehenden Verkehr. Jede Zahl kann bis zu acht Zeichen umfassen.
   - Zwei hexadezimale Zufallszahlen für den SHA1-Algorithmus für die Authentifizierung. Bei einem 160-Bit-Schlüssel muss jede Zahl 40 Zeichen umfassen. Eine Zahl für `dst enigma`, eine Zahl für `dst partym`.
   - Zwei hexadezimale Zufallszahlen für den AES-Algorithmus für die ESP-Verschlüsselung. Bei einem 256-Bit-Schlüssel muss jede Zahl 64 Zeichen umfassen. Eine Zahl für `dst enigma`, eine Zahl für `dst partym`.

   Wenn Sie über einen Generator für Zufallszahlen an Ihren Standort verfügen, verwenden Sie diesen. Alternativ verwenden Sie den Befehl `od.` Anleitungen dazu finden Sie unter „So erzeugen Sie Zufallszahlen auf einem Solaris-System“ auf Seite 543.

2. **Nehmen Sie über die Systemkonsole eines der Systeme die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

   Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh` für eine sichere remote Anmeldung.

   ---

3 Erstellen Sie die SAs

- **Befolgen Sie ab Solaris 10 4/09 Schritt 8 bis Schritt 10.**
- **Wenn Sie mit einer älteren Version als Solaris 10 4/09 arbeiten, befolgen Sie Schritt 4 bis Schritt 9.**

4 Aktivieren Sie den `ipseckey`-Befehlsmodus.

```
# ipseckey

>
```

Die Eingabeaufforderung > kennzeichnet, dass sich das System im `ipseckey`-Befehlsmodus befindet.

5 Wenn Sie vorhandere SAs ersetzen, leeren Sie die aktuellen SAs.

```
> flush
>
```

Um zu verhindern, dass ein potentieller Angreifer die Zeit hat, Ihre SAs zu entschlüsseln, müssen Sie das Schlüsselmaterial ersetzen.

Hinweis – Sie müssen den Schlüsselaustausch jedoch bei kommunizierenden Systemen koordinieren. Wenn Sie die SAs auf einem System ersetzen, müssen sie auch auf dem remoten System ersetzt werden.

---

6 Zum Erstellen von SAs geben Sie den folgenden Befehl ein.

```
> add protocol spi random-hex-string \
src addr dst addr2 \
protocol-prefix_alg protocol-algorithm  \
protocol-prefixkey random-hex-string-of-algorithm-specified-length
```

Sie verwenden diese Syntax auch zum Ersetzen der gerade geleerten SAs.

Protokoll
: Geben Sie entweder `esp` oder `ah` an.

zufällige-hexadezimale-Zeichenfolge
: Gibt eine Zufallszahl mit bis zu acht Zeichen in hexadezimalem Format an. Stellen Sie den Zeichen das Präfix `0x` voran. Wenn Sie mehr Zahlen eingeben, als der Security Parameter Index (SPI) akzeptiert, so ignoriert das System die überflüssigen Zahlen. Wenn Sie weniger Zahlen eingeben als der Security Parameter Index (SPI) akzeptiert, so füllt das System Ihren Eintrag auf.

adr
: Gibt die IP-Adresse eines Systems an.

adr2
Gibt die IP-Adresse des Peer-Systems von *adr* an.

Protokollpräfix
Gibt entweder `encr` oder `auth` an. Das Präfix `encr` wird mit dem `esp`-Protokoll verwendet. Das Präfix `auth` wird mit dem `ah`-Protokoll und zur Authentifizierung des `esp`-Protokolls verwendet.

Protokollalgorithmus
Gibt einen Algorithmus für ESP oder AH an. Jeder Algorithmus erfordert einen Schlüssel mit einer bestimmten Länge.

Die Authentifizierungsalgorithmen umfassen MD5 und SHA1. Ab Version Solaris 10 4/09 werden SHA256 und SHA512 unterstützt. Verschlüsselungsalgorithmen beinhalten DES, 3DES, AES und Blowfish.

zufällige-hexadezimale-Zeichenfolge-in-der-vom-Algorithmus-vorbestimmten-Länge
Gibt eine zufällige hexadezimale Zahl der Länge an, die für den Algorithmus erforderlich ist. Beispielsweise erfordert der MD5-Algorithmus einen 32-Zeichen-String für den 128-Bit-Schlüssel. Der 3DES-Algorithmus erfordert einen 48-Zeichen-String für den 192-Bit-Schlüssel.

a. **Schützen Sie z. B. abgehende Pakete auf dem System `enigma`.**

Verwenden Sie die in Schritt 1 erzeugten Zufallszahlen.

Unter Solaris 10 1/06:

```
> add esp spi 0x8bcd1407 \
src 192.168.116.16 dst 192.168.13.213 \
encr_alg aes \
auth_alg sha1 \
encrkey c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \
authkey 6fab07fec4f2895445500ed992ab48835b9286ff
>
```

Hinweis – Das Peer-System muss das gleiche Schlüsselmaterial und den gleichen SPI verwenden.

---

b. **Bleiben Sie auf dem `enigma`-System im `ipseckey`-Befehlsmodus, und schützen Sie die eingehenden Pakete.**

Geben Sie die folgenden Befehle ein, um die Pakete zu schützen:

```
> add esp spi 0x122a43e4 \
src 192.168.13.213 dst 192.168.116.16 \
encr_alg aes \
auth_alg sha1 \
encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \
authkey c80984bc4733cc0b7c228b9b74b988d2b7467745
>
```

Hinweis – Die Schlüssel und der SPI können für jede SA unterschiedlich sein. Sie *sollten* für jede SA andere Schlüssel und einen anderen SPI zuweisen.

---

7. **Um den `ipseckey`-Befehlsmodus zu beenden, drücken Sie Strg-D oder geben `quit` ein.**

8. **Fügen Sie der `/etc/inet/secret/ipseckeys`-Datei das Schlüsselmaterial hinzu.**

   In älteren Versionen als Solaris 10 4/09 wird durch diesen Schritt sichergestellt, dass IPsec das Schlüsselmaterial beim Neustart zur Verfügung steht.

   Die Zeilen in der `/etc/inet/secret/ipseckeys` sind identisch mit der Befehlszeilensprache `ipseckey`.

   a. **Beispielsweise ähnelt die Datei `/etc/inet/secret/ipseckeys` auf dem `enigma`-System dem Folgenden:**

```
# ipseckeys - This file takes the file format documented in
#   ipseckey(1m).
#   Note that naming services might not be available when this file
#   loads, just like ipsecinit.conf.
#
# for outbound packets on enigma
add esp spi 0x8bcd1407 \
   src 192.168.116.16 dst 192.168.13.213  \
   encr_alg aes \
   auth_alg sha1  \
   encrkey  c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \
   authkey  6fab07fec4f2895445500ed992ab48835b9286ff
#
# for inbound packets
add esp spi 0x122a43e4 \
   src 192.168.13.213 dst 192.168.116.16 \
   encr_alg aes \
   auth_alg sha1  \
   encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \
   authkey c80984bc4733cc0b7c228b9b74b988d2b7467745
```

   b. **Schützen Sie die Datei, indem Sie Nur-Lese-Berechtigungen zuweisen.**

```
# chmod 400 /etc/inet/secret/ipseckeys
```

9. **Wiederholen Sie den Vorgang auf dem System `partym`.**

   Verwenden Sie das gleiche Schlüsselmaterial wie für `enigma`.

   Das Schlüsselmaterial *muss* auf den beiden Systemen identisch sein. Wie in dem folgenden Beispiel gezeigt, unterscheiden sich lediglich die Kommentare in der `ipseckeys`-Datei. Dies ist der Fall, weil `dstenigma` auf dem `enigma`-System für eingehenden Verkehr und auf dem `partym`-System für ausgehenden Verkehr gilt.

```
# partym ipseckeys file
#
# for inbound packets
add esp spi 0x8bcd1407 \
```

```
   src 192.168.116.16 dst 192.168.13.213  \
   encr_alg aes \
   auth_alg sha1  \
   encrkey  c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \
   authkey  6fab07fec4f2895445500ed992ab48835b9286ff
#
# for outbound packets
add esp spi 0x122a43e4 \
   src 192.168.13.213 dst 192.168.116.16 \
   encr_alg aes \
   auth_alg sha1  \
   encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \
   authkey c80984bc4733cc0b7c228b9b74b988d2b7467745
```

10 Aktivieren Sie den Service `manual-key`.

```
# svcadm enable svc:/network/ipsec/manual-key
```

Informationen zum Ersetzen von Schlüsseln in der aktuellen Version finden Sie in Beispiel 20–4.

Beispiel 20–4 Ersetzen von IPsec-SAs

In diesem Beispiel konfiguriert der Administrator ein System, auf dem die aktuelle VersionSolaris 10 ausgeführt wird. Der Administrator generiert neue Schlüssel, ändert die Schlüsselinformationen in der Datei `ipseckeys` und startet den Service dann neu.

- Zunächst generiert der Administrator die Schlüssel nach dem unter „So erzeugen Sie Zufallszahlen auf einem Solaris-System“ auf Seite 543 beschriebenen Verfahren.
- Dann verwendet der Administrator die generierten Schlüssel in der Datei `/etc/inet/secret/ipseckeys`.

  Der Administrator hat dieselben Algorithmen verwendet. Darum ändert der Administrator nur die Werte von `SPI`, `encrkey` und `authkey`:

```
add esp spi 0x8xzy1492 \
   src 192.168.116.16 dst 192.168.13.213  \
   encr_alg aes \
   auth_alg sha1  \
   encrkey 0a1f3886b06ebd7d39f6f89e4c29c93f2741c6fa598a38af969907a29ab1b42a \
   authkey a7230aabf513f35785da73e33b064608be41f69a
#
# add esp spi 0x177xce34\
   src 192.168.13.213 dst 192.168.116.16 \
   encr_alg aes \
   auth_alg sha1  \
   encrkey 4ef5be40bf93498017b2151d788bb37e372f091add9b11149fba42435fefe328 \
   authkey 0e1875d9ff8e42ab652766a5cad49f38c9152821
```

- Schließlich startet der Administrator den `manual-key`-Service neu. Der Neustartbefehl löscht die alten Schlüssel, bevor die neuen Schlüssel hinzugefügt werden.

```
# svcadm restart manual-key
```

▼ So prüfen Sie, ob Pakete mit IPsec geschützt sind

Um zu Überprüfen, ob die Pakete geschützt sind, testen Sie die Verbindung mit dem Befehl `snoop`. In der Ausgabe des Befehls `snoop` können die folgenden Präfixe erscheinen:

- `AH:` Dieses Präfix kennzeichnet, dass die Header durch den AH geschützt sind. Die Ausgabe enthält `AH:` , wenn Sie `auth_alg` zum Schützen des Verkehrs gewählt haben.
- `ESP:` Dieses Präfix kennzeichnet, dass verschlüsselte Daten gesendet werden. Die Ausgabe enthält `ESP:` , wenn Sie `encr_auth_alg` oder `encr_alg` zum Schützen des Verkehrs gewählt haben.

Bevor Sie beginnen Zum Erstellen einer Ausgabe des Befehls `snoop` müssen Sie als Superuser angemeldet sein oder eine entsprechende Rolle angenommen haben. Sie müssen Zugriff auf beide Systeme haben, um die Verbindung zu testen.

1. **Melden Sie sich auf einem System, z. B.** `partym`**, als Superuser an.**

```
% su -
Password:        Type root password
#
```

2. **Bereiten Sie vom** `partym`**-System aus das Snoopen der Pakete von einem remoten System vor.**

Snoopen Sie in einem Terminal-Fenster auf `partym` die Pakete vom `enigma`-System.

```
# snoop -v enigma
Using device /dev/hme (promiscuous mode)
```

3. **Senden Sie ein Paket vom remoten System.**

Melden Sie sich in einem anderen Terminal-Fenster remote beim `enigma`-System an. Geben Sie Ihr Passwort ein. Melden der Sie sich dann als Superuser an und senden Sie ein Paket vom `enigma`-System an das `partym`-System. Das Paket soll von dem Befehl `snoop -venigma` erfasst werden.

```
% ssh enigma
Password:        Type your password
% su -
Password:        Type root password
# ping partym
```

4. **Zeigen Sie die Ausgabe des Befehls** `snoop` **an.**

Auf dem `partym`-die System sollten Sie eine Ausgabe sehen, die `AH`- und `ESP`-Informationen nach den einleitenden `IP`-Header-Informationen enthält. `AH`- und `ESP`-Informationen, die dem Folgenden ähneln, sind geschützte Pakete:

```
IP:   Time to live = 64 seconds/hops
IP:   Protocol = 51 (AH)
IP:   Header checksum = 4e0e
IP:   Source address = 192.168.116.16, enigma
IP:   Destination address = 192.168.13.213, partym
```

```
IP:   No options
IP:
AH:  ----- Authentication Header -----
AH:
AH:  Next header = 50 (ESP)
AH:  AH length = 4 (24 bytes)
AH:  <Reserved field = 0x0>
AH:  SPI = 0xb3a8d714
AH:  Replay = 52
AH:  ICV = c653901433ef5a7d77c76eaa
AH:
ESP:  ----- Encapsulating Security Payload -----
ESP:
ESP:  SPI = 0xd4f40a61
ESP:  Replay = 52
ESP:     ....ENCRYPTED DATA....

ETHER:  ----- Ether Header -----
...
```

▼ How to Configure a Role for Network Security

Wenn Sie die rollenbasierte Zugriffskontrolle (RBAC) zur Verwaltung Ihrer Systeme einsetzen, können Sie mit dem folgenden Verfahren eine Rolle für die Netzwerkverwaltung oder Netzwerksicherheit erstellen.

1. **Suchen Sie das Network-Rechteprofil in der lokalen `prof_attr`-Datenbank.**

   In der aktuellen Version sieht die Ausgabe ungefähr folgendermaßen aus:

```
% cd /etc/security
% grep Network prof_attr
Network IPsec Management:::Manage IPsec and IKE...
Network Link Security:::Manage network link security...
Network Management:::Manage the host and network configuration...
Network Security:::Manage network and host security...
Network Wifi Management:::Manage wifi network configuration...
Network Wifi Security:::Manage wifi network security...
```

   Wenn Sie mit einer älteren Version von Solaris 10 4/09 arbeiten, sieht die Ausgabe ungefähr folgendermaßen aus:

```
% cd /etc/security
% grep Network prof_attr
Network Management:::Manage the host and network configuration
Network Security:::Manage network and host security
System Administrator::: Network Management
```

   Das Network Management-Profil ist ein ergänzendes Profil im System Administrator-Profil. Wenn Sie das System Administrator-Rechteprofil in eine Rolle aufgenommen haben, kann diese Rolle die Befehle im Network Management-Profil ausführen.

2 Stellen Sie fest, welche Befehle im Network Management-Rechteprofil zulässig sind.

```
% grep "Network Management" /etc/security/exec_attr
Network Management:solaris:cmd:::/usr/sbin/ifconfig:privs=sys_net_config
...
Network Management:suser:cmd:::/usr/sbin/snoop:uid=0
```

Die Richtlinienbefehle `solaris` werden mit einer Berechtigung (`privs=sys_net_config`) ausgeführt. Die Richtlinienbefehle `suser` werden als Superuser (`uid=0`) ausgeführt.

3 Legen Sie den Umfang der Netzwerksicherheitsrollen an Ihrem Standort fest.

Verwenden Sie die Definitionen der Rechteprofile in Schritt 1, um eine Entscheidung zu treffen.

- **Zum Erstellen einer Rolle, die sich um die gesamte Netzwerksicherheit kümmert, verwenden Sie das Rechteprofil für Netzwerksicherheit.**
- **In der aktuellen Version verwenden Sie zum Erstellen einer Rolle zur ausschließlichen Verwaltung von IPsec und IKE das Rechteprofil für die Netzwerk-IPsec-Verwaltung.**

4 Erstellen Sie eine Netzwerksicherheitsrolle, die das Rechteprofil für die Netzwerkverwaltung enthält.

Mit einer Rolle mit dem Rechteprofil für Netzwerksicherheit bzw. Netzwerk-IPsec-Verwaltung können zusätzlich zum Profil für die Netzwerkverwaltung unter anderem die Befehle `ifconfig`, `snoop`, `ipsecconf` und `ipseckey` mit entsprechenden Berechtigungen ausgeführt werden.

Zum Erstellen einer Rolle weisen Sie die Rolle einem Benutzer zu und registrieren die Änderungen beim Namen-Service. Lesen Sie dazu „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

Beispiel 20–5 Aufteilen von Netzwerk-Sicherheitsverantwortlichkeiten zwischen Rollen

In diesem Beispiel teilt der Administrator Netzwerk-Sicherheitsverantwortlichkeiten zwischen zwei Rollen auf. Eine Rolle verwaltet die Wifi- und Linksicherheit, während die andere Rolle IPsec und IKE verwaltet. Jede Rolle ist drei Personen zugewiesen, d. h. einer Person pro Schicht.

Die Rollen werden vom Administrator wie folgt erstellt:

- Die erste Rolle erhält die Bezeichnung "LinkWifi".
  - Der Administrator weist der Rolle die Rechteprofile für Netzwerk-Wifi, Netzwerk-Linksicherheit und Netzwerkverwaltung zu.
  - Dann weist der Administrator die LinkWifi-Rolle den entsprechenden Benutzern zu.
- Die zweite Rolle lautet "IPsec-Administrator".
  - Der Administrator weist der Rolle die Rechteprofile für Netzwerk-IPsec-Verwaltung und Netzwerkverwaltung zu.
  - Dann weist der Administrator die IPsec-Administrator-Rolle den entsprechenden Benutzern zu.

▼ Verwalten von IKE- und IPsec-Services

In den folgenden Schritten werden die wahrscheinlichsten Verwendungsmöglichkeiten der SMF-Services für IPsec, IKE und der manuellen Schlüsselverwaltung beschrieben. Die `policy`- und `ipsecalgs`-Services werden standardmäßig aktiviert. Außerdem werden die `ike`- und `manual-key`-Services standardmäßig deaktiviert.

1. **Führen Sie eine der folgenden Aktionen zum Verwalten der IPsec-Richtlinie aus:**

   - **Aktualisieren Sie nach dem Hinzufügen neuer Richtlinien zur Datei** `ipsecinit.conf` **den** `policy`**-Service.**

     ```
     # svcadm refresh svc:/network/ipsec/policy
     ```

   - **Zeigen Sie nach dem Ändern des Wertes einer Serviceeigenschaft den Eigenschaftswert an, und führen Sie eine Aktualisierung und einen Neustart des** `policy`**-Services durch.**

     ```
     # svccfg -s policy setprop config/config_file=/etc/inet/MyIpsecinit.conf
     # svcprop -p config/config_file policy
     /etc/inet/MyIpsecinit.conf
     # svcadm refresh svc:/network/ipsec/policy
     # svcadm restart svc:/network/ipsec/policy
     ```

2. **Führen Sie eine der folgenden Aktionen zum automatischen Verwalten von Schlüsseln durch:**

   - **Aktivieren Sie nach dem Hinzufügen von Einträgen zur Datei** `/etc/inet/ike/config` **den** `ike`**-Service.**

     ```
     # svcadm enable svc:/network/ipsec/ike
     ```

   - **Aktualisieren Sie nach dem Ändern von Einträgen in der Datei** `/etc/inet/ike/config` **den** `ike`**-Service.**

     ```
     # svcadm refresh svc:/network/ipsec/ike
     ```

   - **Zeigen Sie nach dem Ändern des Wertes einer Serviceeigenschaft den Eigenschaftswert an, und führen Sie eine Aktualisierung und einen Neustart des Services durch.**

     ```
     # svccfg -s ike setprop config/admin_privilege=modkeys
     # svcprop -p config/admin_privilege ike
     modkeys
     # svcadm refresh svc:/network/ipsec/ike
     # svcadm restart svc:/network/ipsec/ike
     ```

   - **Deaktivieren Sie den** `ike`**-Service, um ihn anzuhalten.**

     ```
     # svcadm disable svc:/network/ipsec/ike
     ```

3 Führen Sie eine der folgenden Aktionen zum manuellen Verwalten von Schlüsseln durch:

- **Aktivieren Sie nach dem Hinzufügen von Einträgen zur Datei** `/etc/inet/secret/ipseckeys` **den** `manual-key`**-Service.**

  ```
  # svcadm enable svc:/network/ipsec/manual-key
  ```

- **Aktualisieren Sie den Service nach dem Ändern der Datei** `ipseckeys`**.**

  ```
  # svcadm refresh manual-key
  ```

- **Zeigen Sie nach dem Ändern des Wertes einer Serviceeigenschaft den Eigenschaftswert an, und führen Sie eine Aktualisierung und einen Neustart des Services durch.**

  ```
  # svccfg -s manual-key setprop config/config_file=/etc/inet/secret/MyIpseckeyfile
  # svcprop -p config/config_file manual-key
  /etc/inet/secret/MyIpseckeyfile
  # svcadm refresh svc:/network/ipsec/manual-key
  # svcadm restart svc:/network/ipsec/manual-key
  ```

- **Zum Verhindern der manuellen Schlüsselverwaltung deaktivieren Sie den** `manual-key`**-Service.**

  ```
  # svcadm disable svc:/network/ipsec/manual-key
  ```

4 Wenn Sie die IPsec-Protokolle und die Algorithmustabelle ändern, aktualisieren Sie den `ipsecalgs`**-Service.**

```
# svcadm refresh svc:/network/ipsec/ipsecalgs
```

Allgemeine Fehler Verwenden Sie den Befehl `svcs` *Service*, um den Status eines Service zu ermitteln. Wenn sich der Service im `maintenance`-Modus befindet, folgen Sie den Debugging-Vorschlägen in der Ausgabe des Befehls `svcs -x` *Service*.

Schützen eines VPN mit IPsec

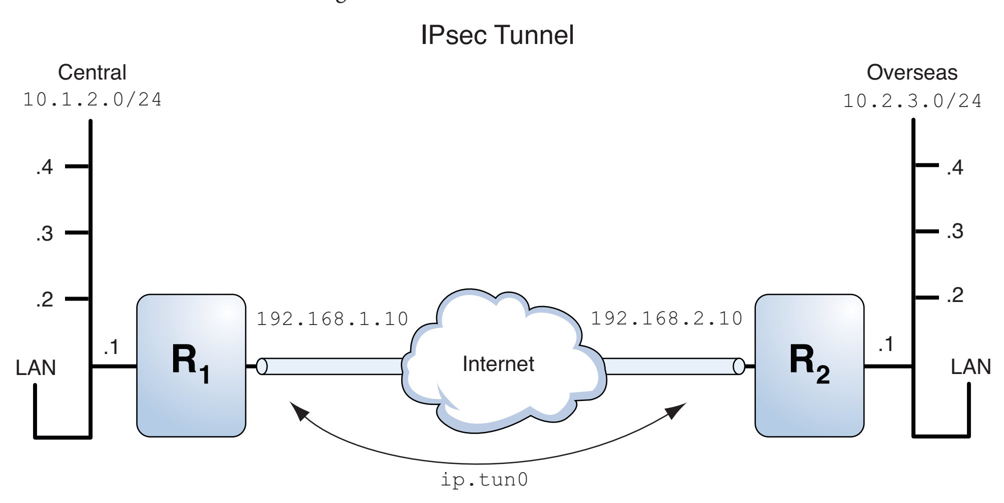
IPsec-Tunnel können ein VPN schützen. Im Release Solaris 10 7/07 kann sich ein Tunnel im Tunnelmodus oder Transportmodus befinden. *Tunnelmodus* kann mit den IPsec-Implementierungen anderer Anbieter zusammenarbeiten. Der *Transportmodus* kann mit früheren Versionen von Solaris OS zusammenarbeiten. Eine Beschreibung der Tunnelmodi finden Sie unter „Transport- und Tunnelmodi in IPsec“ auf Seite 525.

Tunnel im Tunnelmodus bieten eine genauere Kontrolle des Verkehrs. Im Tunnelmodus können Sie für eine interne IP-Adresse den gewünschten Schutz bis hin zu einem einzelnen Port zuweisen.

- Beispiele von IPsec-Richtlinien für Tunnel im Tunnelmodus finden Sie unter „Beispiele für den Schutz eines VPN mit IPsec mithilfe von Tunneln im Tunnelmodus“ auf Seite 555.
- Verfahren zum Schützen von VPNs finden Sie unter „Schützen eines VPN mit IPsec (Übersicht der Schritte) “ auf Seite 557.

Beispiele für den Schutz eines VPN mit IPsec mithilfe von Tunneln im Tunnelmodus

ABBILDUNG 20–1 IPsec-Tunnel-Diagramm



In den folgenden Beispielen wird davon ausgegangen, dass der Tunnel für alle Teilnetze der LANs konfiguriert ist:

```
## Tunnel configuration ##
# Tunnel name is ip.tun0
# Intranet point for the source is 10.1.2.1
# Intranet point for the destination is 10.2.3.1
# Tunnel source is 192.168.1.10
# Tunnel destination is 192.168.2.10
```

BEISPIEL 20–6 Erstellen eines Tunnels, den alle Teilnetze verwenden können

In diesem Beispiel kann der gesamte Verkehr von den lokalen LANs des LAN Central in Abbildung 20–1 über Router 1 zu Router 2 getunnelt werden, dann wird der Verkehr allen lokalen LANs des LAN Overseas zugestellt. Dieser Verkehr wird mit AES verschlüsselt.

```
## IPsec policy ##
{tunnel ip.tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

BEISPIEL 20–7 Erstellen eines Tunnels, der nur zwei Teilnetze miteinander verbindet

In diesem Beispiel wird nur der Verkehr zwischen Teilnetz `10.1.2.0/24` des LAN Central und Teilnetz `10.2.3.0/24` des LAN Overseas getunnelt und verschlüsselt. Da keine weiteren

BEISPIEL 20–7 Erstellen eines Tunnels, der nur zwei Teilnetze miteinander verbindet *(Fortsetzung)*

weiterer IPsec-Richtlinien für Central vorhanden sind, wird Verkehr an Router 1 abgeworfen, wenn das LAN Central versucht, Verkehr für andere LANs über diesen Tunnel zu routen.

```
## IPsec policy ##
{tunnel ip.tun0 negotiate tunnel laddr 10.1.2.0/24 raddr 10.2.3.0/24}
 ipsec {encr_algs aes encr_auth_algs md5 sha1 shared}
```

BEISPIEL 20–8 Erstellen eines Tunnels für E-Mail-Verkehr nur zwischen zwei Teilnetzen

In diesem Beispiel wird ein Tunnel ausschließlich für E-Mail-Verkehr erstellt. Der Verkehr wird von `10.1.2.0/24` des LAN Central an der E-Mail-Server im Teilnetz `10.2.3.0/24` des LAN Overseas zugestellt. Die E-Mails werden mit Blowfish verschlüsselt. Die Richtlinien gelten für den remoten und den lokalen E-Mail-Port. Die Richtlinie `rport` schützt E-Mail, die Central an den remoten E-Mail-Port von Overseas sendet. Die Richtlinie `lport` schützt E-Mail, die Central von Overseas am lokalen Port 25 empfängt.

```
## IPsec policy for email from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 25
 laddr 10.1.2.0/24 raddr 10.2.3.0/24}
 ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

## IPsec policy for email from Overseas to Central ##
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 25
 laddr 10.1.2.0/24 raddr 10.2.3.0/24}
 ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}
```

BEISPIEL 20–9 Erstellen eines Tunnels für den FTP-Verkehr aller Teilnetze

In diesem Beispiel schützt die IPsec-Richtlinie die FTP-Ports in Abbildung 20–1 mit AES für alle Teilnetze des LAN Central zu allen Teilnetzen des LAN Overseas. Diese Konfiguration arbeitet im aktiven FTP-Modus.

```
## IPsec policy for outbound FTP from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 21}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 20}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## IPsec policy for inbound FTP from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 21}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 20}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Schützen eines VPN mit IPsec (Übersicht der Schritte)

Die folgende Tabelle enthält Links zu den Verfahren, mit denen IPsec zum Schutz des Datenverkehrs über das Internet konfiguriert wird. Diese Verfahren richten ein sicheres virtuelles privates Netzwerk (VPN) zwischen zwei Systemen ein, die durch das Internet voneinander getrennt sind. Eine häufige Anwendung dieser Technologie ist das Schützen von Datenverkehr zwischen Heimarbeitern und dem Unternehmensbüro.

Aufgabe	Beschreibung	Siehe
Schützen von Tunnelverkehr im Tunnelmodus über IPv4.	Schützt Datenverkehr im Tunnelmodus zwischen zwei Solaris 10-Systemen; zwei Oracle Solaris-Systemen; oder zwischen einem Solaris 10-System und einem Oracle Solaris Express-System. Auf dem Solaris 10-System muss mindestens die Solaris 10 7/07-Version laufen. Schützt außerdem Datenverkehr im Tunnelmodus zwischen einem Solaris 10-System oder einem Oracle Solaris Express-System und einem System, das auf einer anderen Plattform ausgeführt wird. Auf dem Solaris 10-System muss mindestens die Solaris 10 7/07-Version laufen.	„So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4" auf Seite 560
Schützen vom Tunnelverkehr im Tunnelmodus über IPv6.	Schützt Datenverkehr im Tunnelmodus zwischen zwei Oracle Solaris-Systemen, die das IPv6-Protokoll verwenden.	„So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv6" auf Seite 570
Schützen vom Tunnelverkehr im Transportmodus über IPv4.	Schützt Datenverkehr im Transportmodus zwischen zwei Solaris 10-Systemen; zwei Solaris-Systemen oder zwischen einem Solaris 10-System und einem Oracle Solaris-System. Auf dem Solaris 10-System muss mindestens die Solaris 10 7/07-Version laufen. Schützt außerdem Datenverkehr im Transportmodus zwischen einem System, auf dem eine frühere Version von Solaris OS und Solaris 10 oder ein Oracle Solaris Express-System. läuft. Auf dem Solaris 10-System muss mindestens die Solaris 10 7/07-Version laufen.	„So schützen Sie ein VPN mit einem IPsec-Tunnel im Transportmodus über IPv4" auf Seite 576
	Schützen Sie Datenverkehr durch das Verwenden einer älteren, eingestellten Syntax. Diese Methode eignet sich insbesondere dann, wenn Sie mit einem System kommunizieren, das eine frühere Version von Solaris OS ausführt. Diese Methode vereinfacht das Vergleichen der Konfigurationsdateien auf den zwei Systemen.	Beispiel 20–11 Beispiel 20–16
Schützen vom Tunnelverkehr im Transportmodus über IPv6.	Schützt Datenverkehr im Tunnelmodus zwischen zwei Oracle Solaris-Systemen, die das IPv6-Protokoll verwenden.	„So schützen Sie ein VPN mit einem IPsec-Tunnel im Transportmodus über IPv6" auf Seite 583

Aufgabe	Beschreibung	Siehe
Verhindern von IP-Spoofing.	Erstellt einen SMF-Service, um das System daran zu hindern, ohne Entschlüsselung Pakete über ein VPN der Pakete weiterzuleiten.	„So verhindern Sie IP-Spoofing“ auf Seite 589

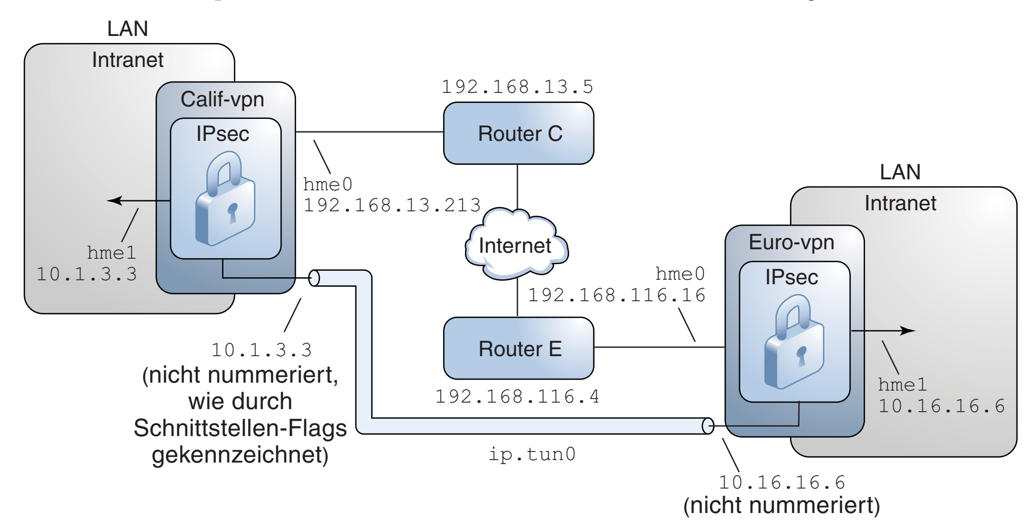
Beschreibung der Netzwerktopologie für IPsec-Aufgaben zum Schützen eines VPN

Bei den in diesem Abschnitt aufgeführten Verfahren wird das im Folgenden beschriebene Setup vorausgesetzt. Eine Darstellung des Netzwerks finden Sie in Abbildung 20–2.

- Jedes System verwendet einen IPv4-Adressraum.

  Ein ähnliches Beispiel mit IPv6-Adressen finden Sie unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv6“ auf Seite 570.
- Jedes System verfügt über zwei Schnittstellen. Die `hme0`-Schnittstelle stellt die Verbindung mit dem Internet her. In diesem Beispiel beginnen die Internet-IP-Adressen mit `192.168`. Die Schnittstelle `hme1` stellt die Verbindung mit dem LAN des Unternehmens, dem Intranet, her. In diesem Beispiel beginnen die Intranet-IP-Adressen mit `10`.
- Jedes System erfordert ESP-Authentifizierung mit dem SHA-1-Algorithmus. Der SHA–1-Algorithmus erfordert einen 160-Bit-Schlüssel.
- Jedes System erfordert ESP-Verschlüsselung mit dem AES-Algorithmus. Der AES-Algorithmus verwendet einen 128-Bit-Schlüssel oder einen 256-Bit-Schlüssel.
- Jedes System kann eine Verbindung zu einem Router herstellen, der über direkten Zugriff auf das Internet verfügt.
- Jedes System verwendet gemeinsam genutzte Sicherheitszuordnungen.

ABBILDUNG 20–2 Beispiel-VPN zwischen Büros, die durch das Internet voneinander getrennt sind



Wie die oben stehende Abbildung zeigt, verwenden die Verfahren für das IPv4-Netzwerk die folgenden Konfigurationsparameter.

Parameter	Europe	California
Systemname	`enigma`	`partym`
System-Intranet-Schnittstelle	`hme1`	`hme1`
Die System-Intranet-Adresse und die *-point*-Adresse in Schritt 7	`10.16.16.6`	`10.1.3.3`
System-Internet-Schnittstelle	`hme0`	`hme0`
Die System-Internet-Adresse und die *tsrc*-Adresse in Schritt 7	`192.168.116.16`	`192.168.13.213`
Name des Internet-Routers	`router-E`	`router-C`
Adresse des Internet-Routers	`192.168.116.4`	`192.168.13.5`
Tunnelname	`ip.tun0`	`ip.tun0`

In den Verfahren werden die folgenden IPv6-Adressen verwendet. Die Tunnelnamen sind dieselben.

Parameter	Europe	California
System-Intranet-Adresse	`6000:6666::aaaa:1116`	`6000:3333::eeee:1113`

Parameter	Europe	California
System-Internet-Adresse	`2001::aaaa:6666:6666`	`2001::eeee:3333:3333`
Adresse des Internet-Routers	`2001::aaaa:0:4`	`2001::eeee:0:1`

▼ So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4

Im Tunnelmodus bestimmt das innere IP-Paket die IPsec-Richtlinie, die dessen Inhalte schützt.

Dieses Verfahren ergänzt das unter „So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec“ auf Seite 535 beschriebene Verfahren. Dieses Setup wird unter „Beschreibung der Netzwerktopologie für IPsec-Aufgaben zum Schützen eines VPN“ auf Seite 558 beschrieben.

Hinweis – Führen Sie die Schritte dieses Verfahrens auf beiden Systemen aus.

Sie verbinden nicht nur zwei Systeme, sondern zwei Intranets, die mit diesen zwei Systemen verbunden sind. Die Systeme in diesem Verfahren arbeiten als Gateways.

Bevor Sie beginnen Sie müssen sich in der globalen Zone befinden, um die IPsec-Richtlinie für das System oder für eine gemeinsame IP-Zone zu konfigurieren. Für eine exklusive IP-Zone konfigurieren Sie die IPsec-Richtlinie in der nicht-globalen Zone.

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh` für eine sichere Remoteanmeldung.

---

2. **Kontrollieren Sie den Paketfluss vor der Konfiguration von IPsec.**

   a. **Stellen Sie sicher, dass IP-Weiterleitung und dynamisches IP-Routing deaktiviert sind.**

```
# routeadm
Configuration       Current          Current
       Option       Configuration  System State
```

```
-----------------------------------------------------
IPv4 forwarding     disabled            disabled
   IPv4 routing     default (enabled)    enabled
...
```

Wenn IP-Weiterleitung und dynamisches IP-Routing aktiviert sind, können diese Funktionen wie folgt deaktiviert werden:

```
# routeadm -d ipv4-routing -d ipv4-forwarding
# routeadm -u
```

Durch Deaktivieren der IP-Weiterleitung wird verhindert, dass Pakete über dieses System von einem Netzwerk zu einem anderen weitergeleitet werden. Eine Beschreibung des Befehls `routeadm` finden Sie in der Manpage `routeadm`(1M).

b. **Aktivieren Sie das IP Strict Destination Multihoming.**

```
# ndd -set /dev/ip ip_strict_dst_multihoming 1
```

Durch Aktivieren von IP Strict Destination Multihoming wird sichergestellt, dass Pakete für eine der Zieladressen auf dem System bei der richtigen Zieladresse eintreffen.

Wenn das Strict Destination Multihoming aktiviert ist, müssen Pakete, die an einer bestimmten Schnittstelle eintreffen, an eine der lokalen IP-Adressen dieser Schnittstelle adressiert sein. Alle anderen Pakete, auch solche, die an andere lokale Adressen des Systems adressiert sind, werden abgeworfen.

Achtung – Der Multihoming-Wert wird beim Booten des Systems auf den Standardwert zurückgesetzt. Informationen zum dauerhaften Ändern des Wertes finden Sie unter „So verhindern Sie IP-Spoofing“ auf Seite 589.

c. **Deaktivieren Sie die meisten Netzwerkservices – wenn möglich, alle Netzwerkservices.**

Hinweis – Wenn Ihr System mit dem SMF-Profil „limited“ installiert wurde, können Sie diesen Schritt überspringen. Netzwerkservices, mit Ausnahme der Solaris Secure Shell, sind deaktiviert.

Durch Deaktivieren der Netzwerkservices wird verhindert, das IP-Pakete Schaden an einem System anrichten können. Beispielsweise könnten ein SNMP-Daemon, eine `telnet`-Verbindung oder eine `rlogin`-Verbindung ausgenutzt werden.

Wählen Sie eine der folgenden Optionen:

- Wenn Sie das Solaris 10 11/06-Release oder eine aktuellere Version ausführen, rufen Sie das SMF-Profil „limited“ auf.

  ```
  # netservices limited
  ```

- Alternativ können Sie die Netzwerkservices einzeln deaktivieren.

```
# svcadm disable network/ftp:default
# svcadm disable network/finger:default
# svcadm disable network/login:rlogin
# svcadm disable network/nfs/server:default
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
```

d. Stellen Sie sicher, dass die meisten Netzwerk-Services deaktiviert sind.

Stellen Sie sicher, dass die Loopback-Mounts und der `ssh`-Service ausgeführt werden.

```
# svcs | grep network
online         Aug_02   svc:/network/loopback:default
...
online         Aug_09   svc:/network/ssh:default
```

3 Fügen Sie zwischen den beiden Systemen zwei SAs hinzu.

Wählen Sie eine der folgenden Optionen:

- Konfiguration von IKE zur Verwaltung der Schlüssel für die SAs. Zur Konfiguration von IKE für das VPN verwenden Sie eines der Verfahren unter „Konfiguration von IKE (Übersicht der Schritte)“ auf Seite 611.
- Wenn ein besonderer Grund vorliegt, die Schlüssel manuell zu konfigurieren, lesen Sie „So erstellen Sie manuell IPsec-Sicherheitszuordnungen“ auf Seite 545.

4 Fügen Sie eine IPsec-Richtlinie hinzu.

Geben Sie die IPsec-Richtlinie für das VPN in die Datei `/etc/inet/ipsecinit.conf` ein. Informationen zur Verstärkung der Richtlinie finden Sie in Beispiel 20–12. Zusätzliche Beispiele finden Sie unter „Beispiele für den Schutz eines VPN mit IPsec mithilfe von Tunneln im Tunnelmodus“ auf Seite 555.

Bei dieser Richtlinie ist der IPsec-Schutz zwischen Systemen im lokalen LAN und mit der internen IP-Adresse des Gateway nicht erforderlich, daher wird eine `bypass`-Anweisung hinzugefügt.

a. Auf dem `enigma`-System geben Sie den folgenden Eintrag in die `ipsecinit.conf`-Datei ein:

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.16.16.6 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. Auf dem `partym`-System geben Sie den folgenden Eintrag in die `ipsecinit.conf`-Datei ein:

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 **(Optional) Überprüfen Sie die Syntax der IPsec-Richtliniendatei.**

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 **Um den Tunnel zu konfigurieren und ihn mit IPsec zu schützen, folgen Sie den Schritten für die jeweilige Solaris-Version:**

- **Folgen Sie ab Solaris 10 4/09 Schritt 7 bis Schritt 13, und führen Sie dann das Routingprotokoll in Schritt 22 aus.**
- **Wenn Sie mit einer älteren Version als Solaris 10 4/09 arbeiten, befolgen Sie Schritt 14 bis Schritt 22.**

7 **Konfigurieren Sie den Tunnel,** `ip.tun0`**, in der Datei** `/etc/hostname.ip.tun0`**.**

Für die Datei gilt folgende Syntax:

system1-point system2-point `tsrc` *system1-taddr* `tdst` *system2-taddr* `router up`

a. **Fügen Sie auf dem System** `enigma` **den folgenden Eintrag in die** `hostname.ip.tun0`**-Datei ein:**

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. **Fügen Sie auf dem System** `partym` **den folgenden Eintrag in die** `hostname.ip.tun0`**-Datei ein:**

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

8 **Schützen Sie den Tunnel mit der von Ihnen erstellten IPsec-Richtlinie.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 **Um den Inhalt der Tunnelkonfigurationsdatei in den Systemkern einzulesen, starten Sie die Netzwerk-Services neu.**

```
# svcadm restart svc:/network/initial:default
```

10 **Aktivieren Sie die IP-Weiterleitung für die** `hme1`**-Schnittstelle.**

a. **Fügen Sie auf dem System** `enigma` **den Routereintrag in die** `/etc/hostname.hme1`**-Datei ein.**

```
192.168.116.16 router
```

b. **Fügen Sie auf dem System** `partym` **den Routereintrag in die** `/etc/hostname.hme1`**-Datei ein:**

```
192.168.13.213 router
```

IP-Weiterleitung bedeutet, dass alle Pakete, unabhängig vom Absender weitergeleitet werden. Darüber hinaus bedeutet IP-Weiterleitung, dass Pakete, die diese Schnittstelle verlassen, möglicherweise von einem anderen Absender stammen. Um ein Paket erfolgreich weiterzuleiten, müssen sowohl die empfangende als auch die übertragende Schnittstelle die IP-Weiterleitung aktiviert haben.

Da die Schnittstelle `hme1` *innerhalb* des Intranets liegt, muss die IP-Weiterleitung für `hme1` aktiviert sein. Da `ip.tun0` die zwei Systeme über das Internet miteinander verbindet, muss die IP-Weiterleitung für `ip.tun0` aktiviert sein.

Jedoch wurde die IP-Weiterleitung für die Schnittstelle `hme0` deaktiviert, um zu verhindern, dass ein Angreifer von *außen* Pakete in das geschützte Intranet einleitet. *außen* bezieht sich in diesem Fall auf das Internet.

11 Stellen Sie sicher, dass die Routing-Protokolle die Standardroute nicht innerhalb des Intranets bekannt geben.

a. **Fügen Sie auf dem System** `enigma` **die** `private`**-Flag in die** `/etc/hostname.hme0`**-Datei ein.**

```
10.16.16.6 private
```

b. **Fügen Sie auf dem System** `partym` **die** `private`**-Flag in die** `/etc/hostname.hme0`**-Datei ein.**

```
10.1.3.3 private
```

Auch wenn die IP-Weiterleitung für die Schnittstelle `hme0` deaktiviert wurde, kann eine Routing-Protokoll-Implementierung die Schnittstelle noch immer bekannt geben. Beispielsweise könnte das `in.routed`-Protokoll bekannt geben, dass `hme0` in der Lage ist, Pakete an ihre Peers im Intranet weiterzuleiten. Durch Einstellen des Schnittstellen-Flags *private* werden diese Advertisement-Nachrichten verhindert.

12 Fügen Sie manuell eine Standardroute über die `hme0`**-Schnittstelle hinzu.**

Die Standardroute muss ein Router mit direktem Zugriff auf das Internet sein.

a. **Auf dem System** `enigma` **können Sie die folgende Route hinzufügen:**

```
# route add default 192.168.116.4
```

b. **Auf dem System** `partym` **fügen Sie die folgende Route hinzu:**

```
# route add default 192.168.13.5
```

Auch wenn die Schnittstelle `hme0` nicht zum Intranet gehört, muss `hme0` über das Internet auf ihr Peer-System zugreifen können. Um ihren Peer zu finden, benötigt die Schnittstelle `hme0` Informationen zum Internet-Routing. Das VPN-System erscheint dem restlichen Internet gegenüber als Host und nicht als Router. Aus diesem Grund können Sie einen Standard-Router verwenden, um das Router-Erkennungsprotokoll zum Finden eines Peer-Systems auszuführen. Weitere Informationen entnehmen Sie bitte den Manpages `route`(1M) and `in.routed`(1M).

13 Zum Schluss wechseln Sie zu Schritt 22, um ein Routingprotokoll auszuführen.

14 Konfigurieren Sie den Tunnel `ip.tun0`**.**

Hinweis – Durch die folgenden Schritte wird ein Tunnel auf einem System konfiguriert, auf dem eine ältere Version als Solaris 10 4/09 ausgeführt wird.

Verwenden Sie `ifconfig`-Befehle, um eine Point-to-Point-Schnittstelle zu erzeugen:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 system1-point system2-point \
tsrc system1-taddr tdst system2-taddr
```

a. **Auf dem System `enigma` geben Sie die folgenden Befehle ein:**

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213
```

b. **Auf dem System `partym` geben Sie die folgenden Befehle ein:**

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.1.3.3 10.16.16.6  \
tsrc 192.168.13.213 tdst 192.168.116.16
```

15. **Schützen Sie den Tunnel mit der von Ihnen erstellten IPsec-Richtlinie.**

```
# ipsecconf
```

16. **Aktivieren Sie den Router für den Tunnel.**

```
# ifconfig ip.tun0 router up
```

17. **Aktivieren Sie die IP-Weiterleitung für die Schnittstelle `hme1`.**

```
# ifconfig hme1 router
```

IP-Weiterleitung bedeutet, dass alle Pakete, unabhängig vom Absender weitergeleitet werden. Darüber hinaus bedeutet IP-Weiterleitung, dass Pakete, die diese Schnittstelle verlassen, möglicherweise von einem anderen Absender stammen. Um ein Paket erfolgreich weiterzuleiten, müssen sowohl die empfangende als auch die übertragende Schnittstelle die IP-Weiterleitung aktiviert haben.

Da die Schnittstelle `hme1` *innerhalb* des Intranets liegt, muss die IP-Weiterleitung für `hme1` aktiviert sein. Da `ip.tun0` die zwei Systeme über das Internet miteinander verbindet, muss die IP-Weiterleitung für `ip.tun0` aktiviert sein.

Jedoch wurde die IP-Weiterleitung für die Schnittstelle `hme0` deaktiviert, um zu verhindern, dass ein Angreifer von *außen* Pakete in das geschützte Intranet einleitet. *außen* bezieht sich in diesem Fall auf das Internet.

18 Stellen Sie sicher, dass die Routing-Protokolle die Standardroute nicht innerhalb des Intranets bekannt geben.

```
# ifconfig hme0 private
```

Auch wenn die IP-Weiterleitung für die Schnittstelle `hme0` deaktiviert wurde, kann eine Routing-Protokoll-Implementierung die Schnittstelle noch immer bekannt geben. Beispielsweise könnte das `in.routed`-Protokoll bekannt geben, dass `hme0` in der Lage ist, Pakete an ihre Peers im Intranet weiterzuleiten. Durch Einstellen des Schnittstellen-Flags *private* werden diese Advertisement-Nachrichten verhindert.

19 Fügen Sie manuell eine Standardroute über `hme0` hinzu.

Die Standardroute muss ein Router mit direktem Zugriff auf das Internet sein.

a. **Auf dem System `enigma` können Sie die folgende Route hinzufügen:**

```
# route add default 192.168.116.4
```

b. **Auf dem System `partym` fügen Sie die folgende Route hinzu:**

```
# route add default 192.168.13.5
```

Auch wenn die Schnittstelle `hme0` nicht zum Intranet gehört, muss `hme0` über das Internet auf ihr Peer-System zugreifen können. Um ihren Peer zu finden, benötigt die Schnittstelle `hme0` Informationen zum Internet-Routing. Das VPN-System erscheint dem restlichen Internet gegenüber als Host und nicht als Router. Aus diesem Grund können Sie einen Standard-Router verwenden, um das Router-Erkennungsprotokoll zum Finden eines Peer-Systems auszuführen. Weitere Informationen entnehmen Sie bitte den Manpages `route`(1M) and `in.routed`(1M).

20 Stellen Sie sicher, dass das VPN nach einem erneuten Booten gestartet wird. Dazu fügen Sie einen Eintrag in die `/etc/hostname.ip.tun0`-Datei ein.

system1-point system2-point `tsrc` *system1-taddr* `tdst` *system2-taddr* `router up`

a. **Fügen Sie auf dem System `enigma` den folgenden Eintrag in die `hostname.ip.tun0`-Datei ein:**

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. **Fügen Sie auf dem System `partym` den folgenden Eintrag in die `hostname.ip.tun0`-Datei ein:**

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

21 Konfigurieren Sie die Schnittstellendateien so, dass die korrekten Parameter an den Routing-Daemon übergeben werden.

a. Ändern Sie auf dem System `enigma` **die** `/etc/hostname.` *Schnittstelle*-**Dateien.**

```
# cat /etc/hostname.hme0
## enigma
10.16.16.6 private

# cat /etc/hostname.hme1
## enigma
192.168.116.16 router
```

b. Ändern Sie auf dem System `partym` **die** `/etc/hostname.` *Schnittstelle*-**Dateien.**

```
# cat /etc/hostname.hme0
## partym
10.1.3.3 private

# cat /etc/hostname.hme1
## partym
192.168.13.213 router
```

22 Führen Sie ein Routingprotokoll aus.

```
# routeadm -e ipv4-routing
# routeadm -u
```

Eventuell müssen Sie das Routing-Protokoll konfigurieren, bevor Sie es ausführen können. Weitere Informationen finden Sie unter „Routing-Protokolle in Oracle Solaris“ auf Seite 273. Anweisungen finden Sie unter „So konfigurieren Sie einen IPv4-Router“ auf Seite 126.

Beispiel 20–10 Erstellen temporärer Tunnels beim Testen

In diesem Beispiel testet der Administrator die Tunnelerstellung auf einem Solaris 10 4/09-System. Später verwendet der Administrator das unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560 Verfahren zur dauerhaften Einrichtung der Tunnel. Während des Testens führt der Administrator eine Reihe von Schritten auf den Systemen `system1` und `system 2` aus.

- Der Administrator führt auf beiden Systemen die ersten fünf Schritte des unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560 erläuterten Verfahrens aus.
- Der Administrator verwendet den `ifconfig`-Befehl zur Untersuchung und Konfiguration eines temporären Tunnels.

```
system1 # ifconfig ip.tun0 plumb
system1 # ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
          tsrc 192.168.116.16 tdst 192.168.13.213

# ssh system2
Password:      admin-password-on-system2
```

```
system2 # ifconfig ip.tun0 plumb
system2 # ifconfig ip.tun0  10.1.3.3 10.16.16.6 \
          tsrc 192.168.13.213 tdst 192.168.116.16
```

- Der Administrator aktiviert die IPsec-Richtlinie für den Tunnel. Die Richtlinie wurde in Schritt 4 des unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560 erläuterten Verfahrens erstellt.

```
system1 # svcadm refresh svc:/network/ipsec/policy:default
system2 # svcadm refresh svc:/network/ipsec/policy:default
```

- Der Administrator wandelt die Internetschnittstelle in einen Router um und verhindert, dass Routingprotokolle über die Intranetschnittstelle hinausgehen.

```
system1 # ifconfig hme1 router ; ifconfig hme0 private

system2 # ifconfig hme1 router ; ifconfig hme0 private
```

- Der Administrator fügt manuell Routing hinzu und führt das Routingprotokoll auf beiden Systemen nach Schritt 12 und Schritt 22 des unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560 beschriebenen Verfahrens aus.

Beispiel 20–11 Erstellen eines Tunnels für eine frühere Version eines Solaris-Systems mithilfe der Befehlszeile

In Solaris 10 7/07 wurde die Syntax des `ifconfig`-Befehls vereinfacht. In diesem Beispiel testet der Administrator die Tunnelerstellung auf einem System, auf dem eine ältere Version als Solaris 10 7/07 ausgeführt wird. Mithilfe der ursprünglichen Syntax des `ifconfig`-Befehls kann der Administrator identische Befehle auf den beiden kommunizierenden Systemen verwenden. Später wandelt der Administrator die Tunnel nach der unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560 erläuterten Verfahrensweise in dauerhafte Tunnel um.

Während des Testens führt der Administrator folgende Schritte auf den Systemen `system1` und `system 2` aus.

- Der Administrator führt auf beiden Systemen die ersten fünf Schritte des unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560 beschriebenen Verfahrens aus.
- Der Administrator untersucht und konfiguriert den Tunnel.

```
system1 # ifconfig ip.tun0 plumb
system1 # ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
          tsrc 192.168.116.16 tdst 192.168.13.213 \
          encr_algs aes encr_auth_algs sha1
system1 # ifconfig ip.tun0 router up

# ssh system2
Password:      admin-password-on-system2
system2 # ifconfig ip.tun0 plumb
system2 # ifconfig ip.tun0 10.1.3.3  10.16.16.6 \
          tsrc 192.168.13.213 tdst 192.168.116.16 \
```

```
          encr_algs aes encr_auth_algs sha1
system2 # ifconfig ip.tun0 router up
```

- Der Administrator aktiviert die IPsec-Richtlinie für den Tunnel. Die Richtlinie wurde in Schritt 4 des unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560 erläuterten Verfahrens erstellt.

```
system1 # svcadm refresh svc:/network/ipsec/policy:default
system2 # svcadm refresh svc:/network/ipsec/policy:default
```

- Der Administrator wandelt die Internetschnittstelle in einen Router um und verhindert, dass Routingprotokolle über die Intranetschnittstelle hinausgehen.

```
system1 # ifconfig hme1 router ; ifconfig hme0 private
system2 # ifconfig hme1 router ; ifconfig hme0 private
```

- Der Administrator fügt Routing nach der in Schritt 12 und Schritt 22 unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560 angegebenen Verfahrensweise auf beiden System hinzu.

Beispiel 20–12 Erfordern einer IPsec-Richtlinie auf allen Systemen in einem LAN

In diesem Beispiel wandelt der Administrator die `bypass`-Richtlinie, die in Schritt 4 konfiguriert wurde, in einen Kommentar um und verstärkt somit den Schutz. Bei dieser Richtlinienkonfiguration muss jedes System im LAN IPsec aktivieren, um mit dem Router kommunizieren zu können.

```
# LAN traffic must implement IPsec.
# {laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel} ipsec {encr_algs aes encr_auth_algs sha1}
```

Beispiel 20–13 Verwenden von IPsec, um Telnet-Verkehr anders als SMTP-Verkehr zu schützen

In diesem Beispiel schützt die erste Regel den `telnet`-Datenverkehr an·Port 23 mit Blowfish und SHA-1. Die zweite Regel schützt den SMTP-Datenverkehr an Port 25 mit AES und MD5.

```
{laddr 10.1.3.3 ulp tcp dport 23 dir both}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa unique}
{laddr 10.1.3.3 ulp tcp dport 25 dir both}
 ipsec {encr_algs aes encr_auth_algs md5 sa unique}
```

Beispiel 20–14 Verwenden eines IPsec-Tunnels im Tunnelmode, um den Teilnetz-Verkehr anders als den restlichen Netzwerkverkehr zu schützen

Die folgende Tunnelkonfiguration schützt den gesamten Verkehr aus dem Teilnetz `10.1.3.0/24` über den Tunnel:

```
{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Die folgende Tunnelkonfiguration schützt Verkehr aus dem Teilnetz `10.1.3.0/24` an andere Teilnetze über den Tunnel. Teilnetze, die mit `10.2.`*x.x* beginnen, befinden sich hinter dem Tunnel.

```
{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.1.0/24}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.2.0/24}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.3.0/24}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

▼ So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv6

Zum Einrichten eines VPN in einem IPv6-Netzwerk führen Sie die gleichen Schritte wie für ein IPv4-Netzwerk aus. Lediglich die Syntax der Befehle ist etwas anders. Eine vollständige Beschreibung der Gründe für bestimmte Befehle finden Sie unter den entsprechenden Schritten der Beschreibung unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560.

Hinweis – Führen Sie die Schritte dieses Verfahrens auf beiden Systemen aus.

In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet.

Parameter	Europe	California
Systemname	`enigma`	`partym`
System-Intranet-Schnittstelle	`hme1`	`hme1`
System-Internet-Schnittstelle	`hme0`	`hme0`
System-Intranet-Adresse	`6000:6666::aaaa:1116`	`6000:3333::eeee:1113`
System-Internet-Adresse	`2001::aaaa:6666:6666`	`2001::eeee:3333:3333`
Name des Internet-Routers	`router-E`	`router-C`
Adresse des Internet-Routers	`2001::aaaa:0:4`	`2001::eeee:0:1`
Tunnelname	`ip6.tun0`	`ip6.tun0`

1 Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh` für eine sichere Remoteanmeldung.

---

2 Kontrollieren Sie den Paketfluss vor der Konfiguration von IPsec.

Informationen zu den Auswirkungen dieser Befehle finden Sie unter Schritt 2 in „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560.

a. Stellen Sie sicher, dass IP-Weiterleitung und dynamisches IP-Routing deaktiviert sind.

```
# routeadm
Configuration       Current         Current
       Option       Configuration  System State
--------------------------------------------------
...
IPv6 forwarding     disabled           disabled
   IPv6 routing     disabled           disabled
```

Wenn IP-Weiterleitung und dynamisches IP-Routing aktiviert sind, können diese Funktionen wie folgt deaktiviert werden:

```
# routeadm -d ipv6-forwarding -d ipv6-routing
# routeadm -u
```

b. Aktivieren Sie das IP Strict Destination Multihoming.

```
# ndd -set /dev/ip ip6_strict_dst_multihoming 1
```

Achtung – `ip_strict_dst_multihoming` wird beim Booten des Systems auf den Standardwert zurückgesetzt. Informationen zum dauerhaften Ändern des Wertes finden Sie unter „So verhindern Sie IP-Spoofing“ auf Seite 589.

---

c. Deaktivieren Sie die meisten Netzwerkservices – wenn möglich, alle Netzwerkservices.

Hinweis – Wenn Ihr System mit dem SMF-Profil „limited“ installiert wurde, können Sie diesen Schritt überspringen. Netzwerkservices, mit Ausnahme der Solaris Secure Shell, sind deaktiviert.

Durch Deaktivieren der Netzwerkservices wird verhindert, das IP-Pakete Schaden an einem System anrichten können. Beispielsweise könnten ein SNMP-Daemon, eine `telnet`-Verbindung oder eine `rlogin`-Verbindung ausgenutzt werden.

Wählen Sie eine der folgenden Optionen:

- Wenn Sie das Solaris 10 11/06-Release oder eine aktuellere Version ausführen, rufen Sie das SMF-Profil „limited" auf.

  ```
  # netservices limited
  ```

- Alternativ können Sie die Netzwerkservices einzeln deaktivieren.

  ```
  # svcadm disable network/ftp:default
  # svcadm disable network/finger:default
  # svcadm disable network/login:rlogin
  # svcadm disable network/nfs/server:default
  # svcadm disable network/rpc/rstat:default
  # svcadm disable network/smtp:sendmail
  # svcadm disable network/telnet:default
  ```

d. Stellen Sie sicher, dass die meisten Netzwerk-Services deaktiviert sind.

Stellen Sie sicher, dass die Loopback-Mounts und der `ssh`-Service ausgeführt werden.

```
# svcs | grep network
online         Aug_02   svc:/network/loopback:default
...
online         Aug_09   svc:/network/ssh:default
```

3 Fügen Sie zwischen den beiden Systemen zwei SAs hinzu.

Wählen Sie eine der folgenden Optionen:

- Konfiguration von IKE zur Verwaltung der Schlüssel für die SAs. Zur Konfiguration von IKE für das VPN verwenden Sie eines der Verfahren unter „Konfiguration von IKE (Übersicht der Schritte)" auf Seite 611.
- Wenn ein besonderer Grund vorliegt, die Schlüssel manuell zu konfigurieren, lesen Sie „So erstellen Sie manuell IPsec-Sicherheitszuordnungen" auf Seite 545.

4 Fügen Sie eine IPsec-Richtlinie für das VPN hinzu.

Geben Sie die IPsec-Richtlinie für das VPN in die Datei `/etc/inet/ipsecinit.conf` ein.

a. Auf dem `enigma`-System geben Sie den folgenden Eintrag in die `ipsecinit.conf`-Datei ein:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic to and from this host can bypass IPsec.
{laddr 6000:6666::aaaa:1116 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate tunnel}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. **Auf dem `partym`-System geben Sie den folgenden Eintrag in die `ipsecinit.conf`-Datei ein:**

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic to and from this host can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate tunnel}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 **(Optional) Überprüfen Sie die Syntax der IPsec-Richtliniendatei.**

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 **Um den Tunnel zu konfigurieren und ihn mit IPsec zu schützen, folgen Sie den Schritten für die jeweilige Solaris-Version:**

- **Folgen Sie ab Solaris 10 4/09 Schritt 7 bis Schritt 13, und führen Sie dann das Routingprotokoll in Schritt 22 aus.**
- **Wenn Sie mit einer älteren Version als Solaris 10 4/09 arbeiten, befolgen Sie Schritt 14 bis Schritt 22.**

7 **Konfigurieren Sie den Tunnel `ip6.tun0` in der `/etc/hostname.ip6.tun0`-Datei.**

a. **Fügen Sie auf dem System `enigma` den folgenden Eintrag in die `hostname6.ip6.tun0`-Datei ein:**

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 router up
```

b. **Fügen Sie auf dem System `partym` den folgenden Eintrag in die `hostname.ip6.tun0`-Datei ein.**

```
6000:3333::eeee:1113  6000:6666::aaaa:1116 tsrc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666 router up
```

8 **Schützen Sie den Tunnel mit der von Ihnen erstellten IPsec-Richtlinie.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 **Um den Inhalt der Tunnelkonfigurationsdatei in den Systemkern einzulesen, starten Sie die Netzwerk-Services neu.**

```
# svcadm restart svc:/network/initial:default
```

10 **Aktivieren Sie die IP-Weiterleitung für die Schnittstelle `hme1`.**

a. **Fügen Sie auf dem System `enigma` den Routereintrag in die `/etc/hostname6.hme1`-Datei ein.**

```
2001::aaaa:6666:6666 inet6 router
```

b. **Fügen Sie auf dem System `partym` den Routereintrag in die `/etc/hostname6.hme1`-Datei ein.**

```
2001::eeee:3333:3333 inet6 router
```

11 **Stellen Sie sicher, dass die Routing-Protokolle die Standardroute nicht innerhalb des Intranets bekannt geben.**

a. **Fügen Sie auf dem System `enigma` die `private`-Flag in die `/etc/hostname6.hme0`-Datei ein.**

```
6000:6666::aaaa:1116 inet6 private
```

b. **Fügen Sie auf dem System `partym` die `private`-Flag in die `/etc/hostname6.hme0`-Datei ein.**

```
6000:3333::eeee:1113 inet6 private
```

12 **Fügen Sie manuell eine Standardroute über `hme0` hinzu.**

a. **Auf dem System `enigma` können Sie die folgende Route hinzufügen:**

```
# route add -inet6 default 2001::aaaa:0:4
```

b. **Auf dem System `partym` fügen Sie die folgende Route hinzu:**

```
# route add -inet6 default 2001::eeee:0:1
```

13 **Zum Schluss wechseln Sie zu Schritt 22, um ein Routingprotokoll auszuführen.**

14 **Konfigurieren Sie den sicheren Tunnel `ip6.tun0`.**

Hinweis – Durch die folgenden Schritte wird ein Tunnel auf einem System konfiguriert, auf dem eine ältere Version als Solaris 10 4/09 ausgeführt wird.

---

a. **Auf dem System `enigma` geben Sie die folgenden Befehle ein:**

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666   tdst 2001::eeee:3333:3333
```

b. **Auf dem System `partym` geben Sie die folgenden Befehle ein:**

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6 6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333   tdst 2001::aaaa:6666:6666
```

15 **Schützen Sie den Tunnel mit der von Ihnen erstellten IPsec-Richtlinie.**

```
# ipsecconf
```

16 **Aktivieren Sie den Router für den Tunnel.**

```
# ifconfig ip6.tun0 router up
```

17 Aktivieren Sie auf jedem System die IP-Weiterleitung für die Schnittstelle `hme1`.

```
# ifconfig hme1 router
```

18 Stellen Sie sicher, dass die Routing-Protokolle die Standardroute nicht innerhalb des Intranets bekannt geben.

```
# ifconfig hme0 private
```

19 Fügen Sie manuell eine Standardroute über `hme0` hinzu.

Die Standardroute muss ein Router mit direktem Zugriff auf das Internet sein.

a. **Auf dem System `enigma` können Sie die folgende Route hinzufügen:**

```
# route add -inet6 default 2001::aaaa:0:4
```

b. **Auf dem System `partym` fügen Sie die folgende Route hinzu:**

```
# route add -inet6 default 2001::eeee:0:1
```

20 Stellen Sie sicher, dass das VPN nach einem erneuten Booten gestartet wird. Dazu fügen Sie einen Eintrag in die `/etc/hostname6.ip6.tun0`-Datei ein.

Dieser Eintrag repliziert die Parameter, die in Schritt 14 an den Befehl `ifconfig` übergeben wurden.

a. **Fügen Sie auf dem System `enigma` den folgenden Eintrag in die `hostname6.ip6.tun0`-Datei ein:**

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666  tdst 2001::eeee:3333:3333 router up
```

b. **Fügen Sie auf dem System `partym` den folgenden Eintrag in die `hostname6.ip6.tun0`-Datei ein:**

```
6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333   tdst 2001::aaaa:6666:6666  router up
```

21 Konfigurieren Sie die Schnittstellendateien auf jedem System so, dass die korrekten Parameter an den Routing-Daemon übergeben werden.

a. **Ändern Sie auf dem System `enigma` die `/etc/hostname6.` *Schnittstelle*-Dateien.**

```
# cat /etc/hostname6.hme0
## enigma
6000:6666::aaaa:1116 inet6 private

#  cat /etc/hostname6.hme1
## enigma
2001::aaaa:6666:6666 inet6 router
```

b. Ändern Sie auf dem System `partym` die `/etc/hostname6.` *Schnittstelle*-Dateien.

```
# cat /etc/hostname6.hme0
## partym
6000:3333::eeee:1113 inet6 private

# cat /etc/hostname6.hme1
## partym
2001::eeee:3333:3333 inet6 router
```

22 Führen Sie ein Routingprotokoll aus.

```
# routeadm -e ipv6-routing
# routeadm -u
```

Eventuell müssen Sie das Routing-Protokoll konfigurieren, bevor Sie es ausführen können. Weitere Informationen finden Sie unter „Routing-Protokolle in Oracle Solaris" auf Seite 273. Anweisungen finden Sie unter „Konfiguration eines IPv6-Routers" auf Seite 191.

▼ So schützen Sie ein VPN mit einem IPsec-Tunnel im Transportmodus über IPv4

Im Transportmodus bestimmt der äußere Header die IPsec-Richtlinie, die das innere IP-Paket schützt.

Dieses Verfahren ergänzt das unter „So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec" auf Seite 535 beschriebene Verfahren. Sie verbinden nicht nur zwei Systeme, sondern zwei Intranets, die mit diesen zwei Systemen verbunden sind. Die Systeme in diesem Verfahren arbeiten als Gateways.

Dieses Verfahren verwendet das unter „Beschreibung der Netzwerktopologie für IPsec-Aufgaben zum Schützen eines VPN" auf Seite 558 beschriebene Setup. Eine vollständige Beschreibung der Gründe für bestimmte Befehle finden Sie unter den entsprechenden Schritten der Beschreibung unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4" auf Seite 560.

Hinweis – Führen Sie die Schritte dieses Verfahrens auf beiden Systemen aus.

---

1 Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh` für eine sichere Remoteanmeldung.

---

2. **Kontrollieren Sie den Paketfluss vor der Konfiguration von IPsec.**

   a. **Stellen Sie sicher, dass IP-Weiterleitung und dynamisches IP-Routing deaktiviert sind.**

```
# routeadm
Configuration       Current          Current
       Option       Configuration   System State
---------------------------------------------------
IPv4 forwarding     disabled           disabled
   IPv4 routing     default (enabled)   enabled
...
```

   Wenn IP-Weiterleitung und dynamisches IP-Routing aktiviert sind, können diese Funktionen wie folgt deaktiviert werden:

```
# routeadm -d ipv4-routing -d ipv4-forwarding
# routeadm -u
```

   b. **Aktivieren Sie das IP Strict Destination Multihoming.**

```
# ndd -set /dev/ip ip_strict_dst_multihoming 1
```

Achtung – `ip_strict_dst_multihoming` wird beim Booten des Systems auf den Standardwert zurückgesetzt. Informationen zum dauerhaften Ändern des Wertes finden Sie unter „So verhindern Sie IP-Spoofing“ auf Seite 589.

---

   c. **Deaktivieren Sie die meisten Netzwerkservices – wenn möglich, alle Netzwerkservices.**

Hinweis – Wenn Ihr System mit dem SMF-Profil „limited“ installiert wurde, können Sie diesen Schritt überspringen. Netzwerkservices, mit Ausnahme der Solaris Secure Shell, sind deaktiviert.

   Durch Deaktivieren der Netzwerkservices wird verhindert, das IP-Pakete Schaden an einem System anrichten können. Beispielsweise könnten ein SNMP-Daemon, eine `telnet`-Verbindung oder eine `rlogin`-Verbindung ausgenutzt werden.

   Wählen Sie eine der folgenden Optionen:

   - Wenn Sie das Solaris 10 11/06-Release oder eine aktuellere Version ausführen, rufen Sie das SMF-Profil „limited“ auf.

```
# netservices limited
```

- Alternativ können Sie die Netzwerkservices einzeln deaktivieren.

```
# svcadm disable network/ftp:default
# svcadm disable network/finger:default
# svcadm disable network/login:rlogin
# svcadm disable network/nfs/server:default
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
```

d. Stellen Sie sicher, dass die meisten Netzwerk-Services deaktiviert sind.

Stellen Sie sicher, dass die Loopback-Mounts und der `ssh`-Service ausgeführt werden.

```
# svcs | grep network
online          Aug_02   svc:/network/loopback:default
...
online          Aug_09   svc:/network/ssh:default
```

3 Fügen Sie zwischen den beiden Systemen zwei SAs hinzu.

Wählen Sie eine der folgenden Optionen:

- Konfiguration von IKE zur Verwaltung der Schlüssel für die SAs. Zur Konfiguration von IKE für das VPN verwenden Sie eines der Verfahren unter „Konfiguration von IKE (Übersicht der Schritte)“ auf Seite 611.
- Wenn ein besonderer Grund vorliegt, die Schlüssel manuell zu konfigurieren, lesen Sie „So erstellen Sie manuell IPsec-Sicherheitszuordnungen“ auf Seite 545.

4 Fügen Sie eine IPsec-Richtlinie hinzu.

Geben Sie die IPsec-Richtlinie für das VPN in die Datei `/etc/inet/ipsecinit.conf` ein. Informationen zur Verstärkung der Richtlinie finden Sie in Beispiel 20–15.

a. Auf dem System `enigma` geben Sie den folgenden Eintrag in die `ipsecinit.conf`-Datei ein:

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.16.16.6 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. Auf dem `partym`-System geben Sie den folgenden Eintrag in die `ipsecinit.conf`-Datei ein:

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 (Optional) Überprüfen Sie die Syntax der IPsec-Richtliniendatei.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 **Um den Tunnel zu konfigurieren und ihn mit IPsec zu schützen, folgen Sie den Schritten für die jeweilige Solaris-Version:**

- **Folgen Sie ab Solaris 10 4/09 Schritt 7 bis Schritt 13, und führen Sie dann das Routingprotokoll in Schritt 22 aus.**
- **Wenn Sie mit einer älteren Version als Solaris 10 4/09 arbeiten, befolgen Sie Schritt 14 bis Schritt 22.**

7 **Konfigurieren Sie den Tunnel `ip.tun0` in der `/etc/hostname.ip.tun0`-Datei.**

a. **Fügen Sie auf dem System `enigma` den folgenden Eintrag in die `hostname.ip.tun0`-Datei ein:**

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. **Fügen Sie auf dem System `partym` den folgenden Eintrag in die `hostname.ip.tun0`-Datei ein:**

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

8 **Schützen Sie den Tunnel mit der von Ihnen erstellten IPsec-Richtlinie.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 **Um den Inhalt der `hostname.ip.tun0`-Datei in den Systemkern zu lesen, starten Sie die Netzwerk-Services neu.**

```
# svcadm restart svc:/network/initial:default
```

10 **Aktivieren Sie die IP-Weiterleitung für die `hme1`-Schnittstelle.**

a. **Fügen Sie auf dem System `enigma` den Routereintrag in `/etc/hostname ein.hme1`-Datei.**

```
192.168.116.16 router
```

b. **Fügen Sie auf dem System `partym` den Routereintrag in `/etc/hostname ein.hme1`-Datei.**

```
192.168.13.213 router
```

11 **Stellen Sie sicher, dass die Routing-Protokolle die Standardroute nicht innerhalb des Intranets bekannt geben.**

a. **Fügen Sie auf dem System `enigma` das `private`-Flag in `/etc/hostname ein.hme0`-Datei.**

```
10.16.16.6 private
```

b. **Fügen Sie auf dem System `partym` das `private`-Flag in `/etc/hostname ein.hme0`-Datei.**

```
10.1.3.3 private
```

12 Fügen Sie manuell eine Standardroute über `hme0` hinzu.

a. Auf dem System `enigma` können Sie die folgende Route hinzufügen:

```
# route add default 192.168.116.4
```

b. Auf dem System `partym` fügen Sie die folgende Route hinzu:

```
# route add default 192.168.13.5
```

13 Zum Schluss wechseln Sie zu Schritt 22, um ein Routingprotokoll auszuführen.

14 Konfigurieren Sie den Tunnel `ip.tun0`.

Hinweis – Durch die folgenden Schritte wird ein Tunnel auf einem System konfiguriert, auf dem eine ältere Version als Solaris 10 4/09 ausgeführt wird.

Verwenden Sie `ifconfig`-Befehle, um eine Point-to-Point-Schnittstelle zu erzeugen:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 system1-point system2-point \
tsrc system1-taddr tdst system2-taddr
```

a. Auf dem System `enigma` geben Sie die folgenden Befehle ein:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213
```

b. Auf dem System `partym` geben Sie die folgenden Befehle ein:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.1.3.3 10.16.16.6  \
tsrc 192.168.13.213 tdst 192.168.116.16
```

15 Schützen Sie den Tunnel mit der von Ihnen erstellten IPsec-Richtlinie.

```
# ipsecconf
```

16 Aktivieren Sie den Router für den Tunnel.

```
# ifconfig ip.tun0 router up
```

17 Aktivieren Sie die IP-Weiterleitung für die Schnittstelle `hme1`.

```
# ifconfig hme1 router
```

18 Stellen Sie sicher, dass die Routing-Protokolle die Standardroute nicht innerhalb des Intranets bekannt geben.

```
# ifconfig hme0 private
```

19 Fügen Sie manuell eine Standardroute über `hme0` hinzu.

Die Standardroute muss ein Router mit direktem Zugriff auf das Internet sein.

```
# route add default router-on-hme0-subnet
```

a. **Auf dem System `enigma` können Sie die folgende Route hinzufügen:**

```
# route add default 192.168.116.4
```

b. **Auf dem System `partym` fügen Sie die folgende Route hinzu:**

```
# route add default 192.168.13.5
```

20 Stellen Sie sicher, dass das VPN nach einem erneuten Booten gestartet wird. Dazu fügen Sie einen Eintrag in die `/etc/hostname.ip.tun0`-Datei ein.

```
system1-point system2-point tsrc system1-taddr \
tdst system2-taddr encr_algs aes encr_auth_algs sha1 router up
```

a. **Fügen Sie auf dem System `enigma` den folgenden Eintrag in die `hostname.ip.tun0`-Datei ein:**

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 \
tdst 192.168.13.213 router up
```

b. **Fügen Sie auf dem System `partym` den folgenden Eintrag in die `hostname.ip.tun0`-Datei ein:**

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 \
tdst 192.168.116.16 router up
```

21 Konfigurieren Sie die Schnittstellendateien so, dass die korrekten Parameter an den Routing-Daemon übergeben werden.

a. **Ändern Sie auf dem System `enigma` die `/etc/hostname.`*Schnittstelle*-Dateien.**

```
# cat /etc/hostname.hme0
## enigma
10.16.16.6 private

# cat /etc/hostname.hme1
## enigma
192.168.116.16 router
```

b. **Ändern Sie auf dem System `partym` die `/etc/hostname.`*Schnittstelle*-Dateien.**

```
# cat /etc/hostname.hme0
## partym
10.1.3.3 private

# cat /etc/hostname.hme1
## partym
192.168.13.213 router
```

22 Führen Sie ein Routingprotokoll aus.

```
# routeadm -e ipv4-routing
# routeadm -u
```

Beispiel 20–15 Erfordern einer IPsec-Richtlinie auf allen Systemen im Transportmodus

IPsec-RichtlinieLAN-BeispielIn diesem Beispiel wandelt der Administrator die bypass-Richtlinie, die in Schritt 4 konfiguriert wurde, in einen Kommentar um und verstärkt somit den Schutz. Bei dieser Richtlinienkonfiguration muss jedes System im LAN IPsec aktivieren, um mit dem Router kommunizieren zu können.

```
# LAN traffic must implement IPsec.
# {laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport} ipsec {encr_algs aes encr_auth_algs sha1}
```

Beispiel 20–16 Verwenden einer eingestellten Syntax zur Konfiguration eines IPsec-Tunnels im Transportmodus

In diesem Beispiel stellt der Administrator eine Verbindung zwischen einem Solaris 10 7/07-System und einem System her, das das Solaris 10-Release ausführt. Aus diesem Grund verwendet der Administrator die Solaris 10-Syntax in der Konfigurationsdatei und nimmt die IPsec-Algorithmen in den Befehl `ifconfig` auf.

Der Administrator verwendet das Verfahren „So schützen Sie ein VPN mit einem IPsec-Tunnel im Transportmodus über IPv4“ auf Seite 576 mit den folgenden Syntaxänderungen.

- Für Schritt 4 lautet die Syntax der `ipsecinit.conf`-Datei folgendermaßen:

  ```
  # LAN traffic to and from this address can bypass IPsec.
  {laddr 10.1.3.3 dir both} bypass {}

  # WAN traffic uses ESP with AES and SHA-1.
  {} ipsec {encr_algs aes encr_auth_algs sha1}
  ```
- Für Schritt 14 bis Schritt 16 lautet die Syntax zum Konfigurieren eines sicheren Tunnels folgendermaßen:

  ```
  # ifconfig ip.tun0 plumb

  # ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
  tsrc 192.168.116.16 tdst 192.168.13.213 \
  encr_algs aes encr_auth_algs sha1

  # ifconfig ip.tun0 router up

  # ifconfig ip.tun0 plumb

  # ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
  tsrc 192.168.116.16 tdst 192.168.13.213 \
  encr_algs aes encr_auth_algs sha1
  ```

Die an die `ifconfig`-Befehle übergebene IPsec-Richtlinie muss der IPsec-Richtlinie in der `ipsecinit.conf`-Datei gleichen. Beim erneuten Booten liest das System die `ipsecinit.conf`-Datei ein, um die Richtlinie zu beziehen.

- Für Schritt 20 lautet die Syntax der `hostname.ip.tun0`-Datei folgendermaßen:

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 \
tdst 192.168.13.213 encr_algs aes encr_auth_algs sha1 router up
```

▼ So schützen Sie ein VPN mit einem IPsec-Tunnel im Transportmodus über IPv6

Zum Einrichten eines VPN in einem IPv6-Netzwerk führen Sie die gleichen Schritte wie für ein IPv4-Netzwerk aus. Lediglich die Syntax der Befehle ist etwas anders. Eine vollständige Beschreibung der Gründe für bestimmte Befehle finden Sie unter den entsprechenden Schritten der Beschreibung unter „So schützen Sie ein VPN mit einem IPsec-Tunnel im Tunnelmodus über IPv4“ auf Seite 560.

Hinweis – Führen Sie die Schritte dieses Verfahrens auf beiden Systemen aus.

In diesem Verfahren werden die folgenden Konfigurationsparameter verwendet.

Parameter	Europe	California
Systemname	`enigma`	`partym`
System-Intranet-Schnittstelle	`hme1`	`hme1`
System-Internet-Schnittstelle	`hme0`	`hme0`
System-Intranet-Adresse	`6000:6666::aaaa:1116`	`6000:3333::eeee:1113`
System-Internet-Adresse	`2001::aaaa:6666:6666`	`2001::eeee:3333:3333`
Name des Internet-Routers	`router-E`	`router-C`
Adresse des Internet-Routers	`2001::aaaa:0:4`	`2001::eeee:0:1`
Tunnelname	`ip6.tun0`	`ip6.tun0`

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh` für eine sichere Remoteanmeldung.

---

2 Kontrollieren Sie den Paketfluss vor der Konfiguration von IPsec.

a. Stellen Sie sicher, dass IP-Weiterleitung und dynamisches IP-Routing deaktiviert sind.

```
# routeadm
Configuration       Current         Current
       Option       Configuration  System State
--------------------------------------------------
...
IPv6 forwarding     disabled          disabled
   IPv6 routing     disabled          disabled
```

Wenn IP-Weiterleitung und dynamisches IP-Routing aktiviert sind, können diese Funktionen wie folgt deaktiviert werden:

```
# routeadm -d ipv6-forwarding -d ipv6-routing
# routeadm -u
```

b. Aktivieren Sie das IP Strict Destination Multihoming.

```
# ndd -set /dev/ip ip6_strict_dst_multihoming 1
```

Achtung – `ip_strict_dst_multihoming` wird beim Booten des Systems auf den Standardwert zurückgesetzt. Informationen zum dauerhaften Ändern des Wertes finden Sie unter „So verhindern Sie IP-Spoofing“ auf Seite 589.

---

c. Stellen Sie sicher, dass die meisten Netzwerk-Services deaktiviert sind.

Stellen Sie sicher, dass die Loopback-Mounts und der `ssh`-Service ausgeführt werden.

```
# svcs | grep network
online         Aug_02   svc:/network/loopback:default
...
online         Aug_09   svc:/network/ssh:default
```

3 Fügen Sie zwischen den beiden Systemen zwei SAs hinzu.

Wählen Sie eine der folgenden Optionen:

- Konfiguration von IKE zur Verwaltung der Schlüssel für die SAs. Zur Konfiguration von IKE für das VPN verwenden Sie eines der Verfahren unter „Konfiguration von IKE (Übersicht der Schritte)“ auf Seite 611.
- Wenn ein besonderer Grund vorliegt, die Schlüssel manuell zu konfigurieren, lesen Sie „So erstellen Sie manuell IPsec-Sicherheitszuordnungen“ auf Seite 545.

4 Fügen Sie eine IPsec-Richtlinie hinzu.

Geben Sie die IPsec-Richtlinie für das VPN in die Datei `/etc/inet/ipsecinit.conf` ein.

a. **Auf dem `enigma`-System geben Sie den folgenden Eintrag in die `ipsecinit.conf`-Datei ein:**

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:6666::aaaa:1116 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate transport}
 ipsec {encr_algs aes encr_auth_algs sha1}
```

b. **Auf dem `partym`-System geben Sie den folgenden Eintrag in die `ipsecinit.conf`-Datei ein:**

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate transport}
 ipsec {encr_algs aes encr_auth_algs sha1}
```

5 (Optional) Überprüfen Sie die Syntax der IPsec-Richtliniendatei.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 Um den Tunnel zu konfigurieren und ihn mit IPsec zu schützen, folgen Sie den Schritten für die jeweilige Solaris-Version:

- **Folgen Sie ab Solaris 10 4/09 Schritt 7 bis Schritt 13, und führen Sie dann das Routingprotokoll in Schritt 22 aus.**
- **Wenn Sie mit einer älteren Version als Solaris 10 4/09 arbeiten, befolgen Sie Schritt 14 bis Schritt 22.**

7 Konfigurieren Sie den Tunnel `ip6.tun0` in der `/etc/hostname.ip6.tun0`-Datei.

a. **Fügen Sie auf dem System `enigma` den folgenden Eintrag in die `hostname6.ip6.tun0`-Datei ein:**

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 router up
```

b. **Fügen Sie auf dem System `partym` den folgenden Eintrag in die `hostname.ip6.tun0`-Datei ein.**

```
6000:3333::eeee:1113  6000:6666::aaaa:1116 tsrc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666 router up
```

8 Schützen Sie den Tunnel mit der von Ihnen erstellten IPsec-Richtlinie.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 Um den Inhalt der `hostname.ip6.tun0`-Datei in den Systemkern zu lesen, starten Sie die Netzwerk-Services neu.

```
# svcadm restart svc:/network/initial:default
```

10 Aktivieren Sie die IP-Weiterleitung für die Schnittstelle `hme1`.

a. Fügen Sie auf dem System `enigma` den Routereintrag in die `/etc/hostname6.hme1`-Datei ein.

```
2001::aaaa:6666:6666 inet6 router
```

b. Fügen Sie auf dem System `partym` den Routereintrag in die `/etc/hostname6.hme1`-Datei ein.

```
2001::eeee:3333:3333 inet6 router
```

11 Stellen Sie sicher, dass die Routing-Protokolle die Standardroute nicht innerhalb des Intranets bekannt geben.

a. Fügen Sie auf dem System `enigma` die `private`-Flag in die `/etc/hostname6.hme0`-Datei ein.

```
6000:6666::aaaa:1116 inet6 private
```

b. Fügen Sie auf dem System `partym` die `private`-Flag in die `/etc/hostname6.hme0`-Datei ein.

```
6000:3333::eeee:1113 inet6 private
```

12 Fügen Sie manuell eine Standardroute über `hme0` hinzu.

a. Auf dem System `enigma` können Sie die folgende Route hinzufügen:

```
# route add -inet6 default 2001::aaaa:0:4
```

b. Auf dem System `partym` fügen Sie die folgende Route hinzu:

```
# route add -inet6 default 2001::eeee:0:1
```

13 Zum Schluss wechseln Sie zu Schritt 22, um ein Routingprotokoll auszuführen.

14 Konfigurieren Sie den sicheren Tunnel `ip6.tun0`.

Hinweis – Durch die folgenden Schritte wird ein Tunnel auf einem System konfiguriert, auf dem eine ältere Version als Solaris 10 4/09 ausgeführt wird.

---

a. Auf dem System `enigma` geben Sie die folgenden Befehle ein:

```
# ifconfig ip6.tun0 inet6 plumb
```

```
# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666   tdst 2001::eeee:3333:3333
```

b. **Auf dem System `partym` geben Sie die folgenden Befehle ein:**

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6  6000:3333::eeee:1113  6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333   tdst 2001::aaaa:6666:6666
```

15 **Schützen Sie den Tunnel mit der von Ihnen erstellten IPsec-Richtlinie.**

```
# ipsecconf
```

16 **Aktivieren Sie den Router für den Tunnel.**

```
# ifconfig ip6.tun0 router up
```

17 **Aktivieren Sie die IP-Weiterleitung für die Schnittstelle `hme1`.**

```
# ifconfig hme1 router
```

18 **Stellen Sie sicher, dass die Routing-Protokolle die Standardroute nicht innerhalb des Intranets bekannt geben.**

```
# ifconfig hme0 private
```

19 **Fügen Sie auf jedem System manuell eine Standardroute über `hme0` hinzu.**

Die Standardroute muss ein Router mit direktem Zugriff auf das Internet sein.

a. **Auf dem System `enigma` können Sie die folgende Route hinzufügen:**

```
# route add -inet6 default 2001::aaaa:0:4
```

b. **Auf dem System `partym` fügen Sie die folgende Route hinzu:**

```
# route add -inet6 default 2001::eeee:0:1
```

20 **Stellen Sie auf jedem System sicher, dass das VPN nach einem erneuten Booten gestartet wird. Dazu fügen Sie einen Eintrag in die `/etc/hostname6.ip6.tun0`-Datei ein.**

Dieser Eintrag repliziert die Parameter, die in `Schritt` 14 an den Befehl Schritt 14 übergeben wurden.

a. **Fügen Sie auf dem System `enigma` den folgenden Eintrag in die `hostname6.ip6.tun0`-Datei ein:**

```
6000:6666::aaaa:1116  6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666   tdst 2001::eeee:3333:3333  router up
```

b. **Fügen Sie auf dem System `partym` den folgenden Eintrag in die `hostname6.ip6.tun0`-Datei ein:**

```
6000:3333::eeee:1113  6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333   tdst 2001::aaaa:6666:6666  router up
```

21 Konfigurieren Sie die Schnittstellendateien so, dass die korrekten Parameter an den Routing-Daemon übergeben werden.

a. Ändern Sie auf dem System `enigma` **die** `/etc/hostname6.` *Schnittstelle*-**Dateien.**

```
# cat /etc/hostname6.hme0
## enigma
6000:6666::aaaa:1116 inet6 private

#  cat /etc/hostname6.hme1
## enigma
2001::aaaa:6666:6666 inet6 router
```

b. Ändern Sie auf dem System `partym` **die** `/etc/hostname6.` *Schnittstelle*-**Dateien.**

```
# cat /etc/hostname6.hme0
## partym
6000:3333::eeee:1113 inet6 private

# cat /etc/hostname6.hme1
##
partym2001::eeee:3333:3333 inet6 router
```

22 Führen Sie ein Routingprotokoll aus.

```
# routeadm -e ipv6-routing
# routeadm -u
```

Beispiel 20–17 Verwenden einer eingestellten Syntax zur Konfiguration von IPsec im Transportmodus über IPv6

In diesem Beispiel stellt der Administrator eine Verbindung zwischen einem Solaris 10 7/07-System und einem System her, das das Solaris 10-Release ausführt. Aus diesem Grund verwendet der Administrator die Solaris 10-Syntax in der Konfigurationsdatei und nimmt die IPsec-Algorithmen in den Befehl `ifconfig` auf.

Der Administrator verwendet das Verfahren „So schützen Sie ein VPN mit einem IPsec-Tunnel im Transportmodus über IPv6“ auf Seite 583 mit den folgenden Syntaxänderungen.

- Für Schritt 4 lautet die Syntax der `ipsecinit.conf`-Datei folgendermaßen:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{} ipsec {encr_algs aes encr_auth_algs sha1}
```

- Für Schritt 14 bis Schritt 17 lautet die Syntax zum Konfigurieren eines sicheren Tunnels folgendermaßen:

```
# ifconfig ip6.tun0 inet6 plumb
```

```
# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 \
encr_algs aes encr_auth_algs sha1

# ifconfig ip6.tun0 inet6 router up
```

Die an die `ifconfig`-Befehle übergebene IPsec-Richtlinie muss der IPsec-Richtlinie in der `ipsecinit.conf`-Datei gleichen. Beim erneuten Booten liest das System die `ipsecinit.conf`-Datei ein, um die Richtlinie zu beziehen.

- Für Schritt 20 lautet die Syntax der `hostname6.ip6.tun0`-Datei folgendermaßen:

```
6000:6666::aaaa:1116  6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666   tdst 2001::eeee:3333:3333 \
encr_algs aes encr_auth_algs sha1 router up
```

▼ So verhindern Sie IP-Spoofing

Um IP-Spoofing auszuschließen, muss das System daran gehindert werden, Pakete ohne Entschlüsselung an eine andere Schnittstelle weiterzuleiten. Eine Methode ist das Festlegen der strengen IP-Ziel-Multihoming-Parameter mithilfe des Befehls `ndd`. Wird dieser Parameter in einem SMF-Manifest festgelegt, wird er beim erneuten Booten des Systems eingestellt.

Hinweis – Führen Sie die Schritte dieses Verfahrens auf beiden Systemen aus.

---

1 Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Erstellen Sie das standortspezifische SMF-Manifest zur Verhinderung von IP-Spoofing.

Verwenden Sie das Beispielskript `/var/svc/manifest/site/spoof_check.xml`.

```
<?xml version="1.0"?>
<!DOCTYPE service_bundle SYSTEM "/usr/share/lib/xml/dtd/service_bundle.dtd.1">

<service_bundle type='manifest' name='Custom:ip_spoof_checking'>

<!--    This is a custom smf(5) manifest for this system. Place this
        file in /var/svc/manifest/site, the directory for local
        system customizations. The exec method uses an unstable
        interface to provide a degree of protection against IP
        spoofing attacks when this system is acting as a router.

        IP spoof protection can also be achieved by using ipfilter(5).
        If ipfilter is configured, this service can be disabled.
```

```
        Note: Unstable interfaces might be removed in later
        releases.  See attributes(5).
-->

<service
        name='site/ip_spoofcheck'
        type='service'
        version='1'>

        <create_default_instance enabled='false' />
        <single_instance />

        <!--    Don't enable spoof protection until the
                network is up.
        -->
        <dependency
                name='basic_network'
                grouping='require_all'
                restart_on='none'
                type='service'>
        <service_fmri value='svc:/milestone/network' />
        </dependency>

        <exec_method
                type='method'
                name='start'
                exec='/usr/sbin/ndd -set /dev/ip ip_strict_dst_multihoming 1'
<!--
     For an IPv6 network, use the IPv6 version of this command, as in:
                exec='/usr/sbin/ndd -set /dev/ip ip6_strict_dst_multihoming 1
-->
                timeout_seconds='60'
        />

        <exec_method
                type='method'
                name='stop'
                exec=':true'
                timeout_seconds='3'
        />

        <property_group name='startd' type='framework'>
                <propval
                        name='duration'
                        type='astring'
                        value='transient'
                />
        </property_group>

        <stability value='Unstable' />

</service>
</service_bundle>
```

3 Importieren Sie dieses Manifest in das SMF-Repository.

```
# svccfg import /var/svc/manifest/site/spoof_check.xml
```

4 **Aktivieren Sie den** `ip_spoofcheck`**-Service.**

Verwenden Sie den Namen, der im Manifest `/site/ip_spoofcheck` definiert wird.

```
# svcadm enable /site/ip_spoofcheck
```

5 **Stellen Sie sicher, dass der** `ip_spoofcheck`**-Service online ist.**

```
# svcs /site/ip_spoofcheck
```

KAPITEL 21

IP Security Architecture (Referenz)

Dieses Kapitel enthält die folgenden Referenzinformationen:

- „IPsec Service Management Facility“ auf Seite 593
- „ipsecconf-Befehl“ auf Seite 594
- „ipsecinit.conf-Datei“ auf Seite 595
- „ipsecalgs-Befehl“ auf Seite 597
- „Sicherheitszuordnung-Datenbank für IPsec“ auf Seite 597
- „Dienstprogramme zur Schlüsselerzeugung in IPsec“ auf Seite 598
- „IPsec-Erweiterungen für andere Dienstprogramme“ auf Seite 599

Anweisungen zur Implementierung von IPsec in Ihrem Netzwerk finden Sie in Kapitel 20, „Konfiguration von IPsec (Aufgaben)“. Eine Übersicht zu IPsec finden Sie in Kapitel 19, „IP Security Architecture (Übersicht)“.

IPsec Service Management Facility

Die Service Management Facility (SMF) stellt IPsec die folgenden Services zur Verfügung:

- `svc:/network/ipsec/policy`-**Service** – Zur Verwaltung der IPsec-Richtlinie. Dieser Service ist standardmäßig aktiviert. Der Wert der `config_file`-Eigenschaft bestimmt den Speicherort der `ipsecinit.conf`-Datei. Der anfängliche Wert lautet `/etc/inet/ipsecinit.conf`.
- `svc:/network/ipsec/ipsecalgs` -**Service** – Verwaltet die IPsec zur Verfügung stehenden Algorithmen. Dieser Service ist standardmäßig aktiviert.
- `svc:/network/ipsec/manual-key`-**Service** – Aktiviert das manuelle Schlüsselmanagement. Dieser Service ist standardmäßig deaktiviert. Der Wert der `config_file`-Eigenschaft bestimmt den Speicherort der `ipseckeys`-Konfigurationsdatei. Der anfängliche Wert lautet `/etc/inet/secret/ipseckeys`.

- svc:/network/ipsec/ike-**Service –** Zur IKE-Verwaltung. Dieser Service ist standardmäßig deaktiviert. Informationen zu den konfigurierbaren Eigenschaften finden Sie unter „IKE Service Management Facility" auf Seite 657.

Weitere Informationen zur SMF finden Sie in Kapitel 18, „Managing Services (Overview)" in *System Administration Guide: Basic Administration*. Lesen Sie hierzu auch die Manpages smf(5), svcadm(1M) und svccfg(1M).

ipsecconf-**Befehl**

Mit dem ipsecconf-Befehl wird die IPsec-Richtlinie für einen Host konfiguriert. Wenn Sie diesen Befehl zur Konfiguration der Richtlinie ausführen, erstellt das System IPsec-Richtlinieneinträge im Kernel. Das System verwendet diese Einträge, um die Richtlinie an allen eingehenden und abgehenden IP-Datagrammen zu prüfen. Weitergeleitete Datagramme sind jedoch von den Richtlinienprüfungen, ausgenommen, die mit diesem Befehl hinzugefügt werden. Mit dem Befehl ipsecconf wird auch die Security Policy Database (SPD) konfiguriert.

- Weitere Informationen zum Schützen von weitergeleiteten Paketen finden Sie in den Manpages ifconfig(1M) und tun(7M).
- Optionen für die IPsec-Richtlinie finden Sie in der Manpage ipsecconf(1M).
- Anweisungen zum Verwenden des ipsecconf-Befehls zum Schützen von Datenverkehr zwischen Systemen finden Sie unter „Konfiguration von IKE (Übersicht der Schritte)" auf Seite 611.

Zum Aufrufen des ipsecconf-Befehls müssen Sie sich als Superuser anmelden oder eine entsprechende Rolle annehmen. Der Befehl akzeptiert Einträge, die den Datenverkehr in beide Richtungen schützen, und Einträge, die den Datenverkehr nur in eine Richtung schützen.

Richtlinieneinträge im Format lokale Adresse und remote Adresse können den Datenverkehr mit nur einem Richtlinieneintrag in beiden Richtungen schützen. Beispielsweise schützen Einträge nach dem Muster laddr host1 und raddr host2 Datenverkehr in beiden Richtungen, wenn keine Richtung für den benannten Host angegeben ist. Aus diesem Grund benötigen Sie für jeden Host nur einen Richtlinieneintrag.

Richtlinieneinträge im Format Quelladresse zu Zieladresse schützen Datenverkehr nur in eine Richtung. Beispielsweise schützt ein Richtlinieneintrag nach dem Muster saddr host1 daddr host2 entweder eingehenden Datenverkehr oder abgehenden Datenverkehr, aber keinen bidirektionalen Datenverkehr. Daher müssen Sie, um Datenverkehr in beide Richtungen zu schützen, den Befehl ipsecconf in einem weiteren Eintrag übergeben, z. B. saddr host2 daddr host1.

Um sicherzustellen, dass die IPsec-Richtlinie beim Booten des Computers aktiviert wird, können Sie eine IPsec-Richtliniendatei, /etc/inet/ipsecinit.conf, erstellen. Die Datei wird

beim Starten der Netzwerkservices eingelesen. Anweisungen zum Erstellen einer IPsec-Richtliniendatei finden Sie unter „Schützen des Datenverkehrs mit IPsec (Übersicht der Schritte)“ auf Seite 533.

Ab Solaris 10 4/09 kann mit der `-c`-Option beim `ipsecconf`-Befehl die Syntax der als Argument bereitgestellten IPsec-Richtliniendaten überprüft werden.

Richtlinieneinträge, die über den `ipsecconf`-Befehl hinzugefügt werden, bleiben nicht über einen erneuten Bootvorgang im System erhalten. Damit die IPsec-Richtlinie beim Booten des Systems aktiv ist, müssen die entsprechenden Einträge in die Datei `/etc/inet/ipsecinit.conf` eingefügt werden. Aktualisieren bzw. aktivieren Sie in der aktuellen Version den `policy`-Service. In einer älteren Version als Solaris 10 4/09 müssen Sie das System erneut booten oder den Befehl `ipsecconf` verwenden. Beispiele finden Sie unter „Schützen des Datenverkehrs mit IPsec (Übersicht der Schritte)“ auf Seite 533.

`ipsecinit.conf`-Datei

Um die IPsec-Sicherheitsrichtlinien beim Starten des Solaris OS (Solaris OS) aufzurufen, erstellen Sie eine Konfigurationsdatei, um IPsec mit Ihren speziellen IPsec-Richtlinieneinträgen zu initialisieren. Der Standardname für diese Datei lautet `/etc/inet/ipsecinit.conf`. Ausführliche Informationen zu Richtlinieneinträgen und deren Format finden Sie in der Manpage `ipsecconf(1M)`. Nachdem die Richtlinien konfiguriert sind, können Sie den Befehl `ipsecconf` aufrufen, um die bestehende Konfiguration anzuzeigen oder zu ändern. Ab Solaris 10 4/09 wird die vorhandene Konfiguration durch eine Aktualisierung des `policy`-Service geändert.

Beispiel einer `ipsecinit.conf`-Datei

Die Solaris-Software enthält ein Beispiel einer IPsec-Richtliniendatei, `ipsecinit.sample`. Sie können diese Datei als Vorlage verwenden, um Ihre eigene `ipsecinit.conf`-Datei zu erstellen. Die Datei `ipsecinit.sample` enthält die folgenden Beispiele:

```
#
# For example,
#
#     {rport 23} ipsec {encr_algs des encr_auth_algs md5}
#
# will protect the telnet traffic originating from the host with ESP using
# DES and MD5. Also:
#
#     {raddr 10.5.5.0/24} ipsec {auth_algs any}
#
# will protect traffic to or from the 10.5.5.0 subnet with AH
# using any available algorithm.
#
#
```

```
# To do basic filtering, a drop rule may be used. For example:
#
#     {lport 23 dir in} drop {}
#     {lport 23 dir out} drop {}
# will disallow any remote system from telnetting in.
#
# If you are using IPv6, it may be useful to bypass neighbor discovery
# to allow in.iked to work properly with on-link neighbors. To do that,
# add the following lines:
#
#        {ulp ipv6-icmp type 133-137 dir both } pass { }
#
# This will allow neighbor discovery to work normally.
```

Sicherheitsbetrachtungen für ipsecinit.conf und ipsecconf

Seien Sie vorsichtig, wenn Sie eine Kopie der `ipsecinit.conf`-Datei über ein Netzwerk übertragen. Ein potentieller Angreifer kann eine über das Netzwerk eingehängte Datei lesen, wenn die Datei eingelesen wird. Angenommen, die Datei `/etc/inet/ipsecinit.conf` wird geöffnet oder von einem NFS eingehängten Dateisystem kopiert, kann ein potentieller Angreifer die in der Datei enthaltene Richtlinie ändern.

Stellen Sie sicher, dass Sie IPsec-Richtlinien einrichten, bevor Sie eine Kommunikation initiieren, da bestehende Verbindungen durch Hinzufügen von neuen Richtlinieneinträgen beeinflusst werden können. Entsprechend sollten Sie keine Richtlinien während der Kommunikation ändern.

Eine IPsec-Richtlinie kann insbesondere nicht für SCTP-, TCP- oder UDP-Sockets geändert werden, für die ein `connect()`- oder `accept()`-Funktionsaufruf ausgegeben wurde. Ein Socket, dessen Richtlinie nicht geändert werden kann, wird als *gesperrtes Socket* bezeichnet. Neue Richtlinieneinträge schützen keine Sockets, die bereits gesperrt sind. Weitere Informationen finden Sie in den Manpages `connect`(3SOCKET) und `accept`(3SOCKET).

Schützen Sie Ihr Benennungssystem. Wenn die folgenden beiden Bedingungen erfüllt sind, sind Ihre Hostnamen nicht mehr vertrauenswürdig:

- Ihre Quelladresse ist ein Host, der über das Netzwerk nachgeschlagen werden kann.
- Ihr Benennungssystem wurde kompromittiert.

Sicherheitsschwächen beruhen häufig auf dem Fehlverhalten von Tools, nicht von tatsächlichen Tools. Aus diesem Grund sollten Sie bei der Verwendung des `ipsecconf`-Befehls vorsichtig sein. Verwenden Sie eine Konsole oder ein anderes festverdrahtetes TTY für den sichersten Betriebsmodus.

ipsecalgs-Befehl

Das Solaris Cryptographic Framework bietet Authentifizierungs- und Verschlüsselungsalgorithmen für IPsec. Mit dem ipsecalgs -Befehl werden die Algorithmen aufgeführt, die von den einzelnen IPsec-Protokollen unterstützt werden. Die ipsecalgs-Konfiguration wird in der Datei /etc/inet/ipsecalgs gespeichert. Diese Datei muss in der Regel nicht geändert werden. Wenn Sie sie doch ändern müssen, verwenden Sie den ipsecalgs-Befehl. Diese Datei darf nicht direkt bearbeitet werden. In der aktuellen Version werden die unterstützten Algorithmen beim Booten des Systems mittels des svc:/network/ipsec/ipsecalgs:default-Service mit dem Systemkern synchronisiert.

Die gültigen IPsec-Protokolle und -Algorithmen werden von der ISAKMP-Domain of Interpretation (DOI) beschrieben, die in RFC 2407 behandelt wird. Im allgemeinen Sinn definiert eine DOI Datenformate, Netzverkehr-Austauscharten sowie Konventionen für das Benennen sicherheitsrelevanter Informationen. Bespiele für sicherheitsrelevante Informationen sind Sicherheitsrichtlinien, kryptografische Algorithmen und Kryptographiemodi.

Insbesondere definiert die ISAKMP DOI die Benennungs- und Nummerierungskonventionen für gültige IPsec-Algorithmen und deren Protokolle, PROTO_IPSEC_AH und PROTO_IPSEC_ESP. Jedem Algorithmus ist exakt ein Protokoll zugeordnet. Diese ISAKMP DOI-Definitionen sind in der /etc/inet/ipsecalgs-Datei enthalten. Der Algorithmus und die Protokollnummern werden von der Internet Assigned Numbers Authority (IANA) definiert. Mit dem Befehl ipsecalgs kann die Algorithmenliste für IPsec erweitert werden.

Weitere Informationen zu Algorithmen finden Sie in der Manpage ipsecalgs(1M) Weitere Informationen zum Solaris Cryptographic Framework finden Sie in Kapitel 13, „Oracle Solaris Cryptographic Framework (Overview)“ in *System Administration Guide: Security Services*.

Sicherheitszuordnung-Datenbank für IPsec

Informationen zum Schlüsselmaterial für die IPsec-Sicherheitsservices werden in einer Sicherheitszuordnung-Datenbank (SADB) verwaltet. Sicherheitszuordnungen (SAs) schützen eingehende und abgehende Pakete. Die SADBs werden von einem Benutzerprozess, eventuell von mehreren kooperierenden Prozessen verwaltet, die Nachrichten über einen besonderen Socket senden. Diese Methode der SADBs-Verwaltung entspricht der in Manpage route(7P) beschriebenen Methode. Nur Superuser oder Benutzer, die eine entsprechende Rolle angenommen haben, können auf die Datenbank zugreifen.

Der in.iked-Daemon und der ipseckey-Befehl können die SADBs über die PF_KEY-Socket-Schnittstelle verwalten. Weitere Informationen zur Verarbeitung von Anforderungen und Nachrichten durch die SADBs finden Sie in der Manpage pf_key(7P).

Dienstprogramme zur Schlüsselerzeugung in IPsec

Das IKE-Protokoll bietet ein automatisches Schlüsselmanagement für IPv4- und IPv6-Adressen. Informationen zum Einrichten von IKE finden Sie in Kapitel 23, „Konfiguration von IKE (Aufgaben)“. Das manuelle Schlüssel-Dienstprogramm ist der Befehl `ipseckey`, der in der Manpage `ipseckey(1M)` ausführlich beschrieben wird.

Mit dem `ipseckey`-Befehl können Sie die Datenbank mit den Sicherheitszuordnungen (SADB) manuell auffüllen. In der Regel werden Sicherheitszuordnungen manuell erstellt, wenn IKE nicht zur Verfügung steht. Bei eindeutigen SPI-Werten können die manuelle SA-Erstellung und IKE jedoch auch parallel eingesetzt werden.

Mit dem `ipseckey`-Befehl können alle im System bekannten SAs aufgerufen werden – unabhängig davon, ob die Schlüssel manuell oder mit IKE hinzugefügt wurden. Ab Solaris 10 4/09 kann mit der `-c`-Option des `ipseckey`-Befehls die Syntax der als Argument bereitgestellten Schlüsseldatei überprüft werden.

IPsec-SAs, die mit dem `ipseckey`-Befehl hinzugefügt wurden, gehen bei einem erneuten Booten des Systems verloren. Wenn Sie in der aktuellen Version manuell hinzugefügte SAs beim Booten des Systems aktivieren möchten, fügen Sie Einträge in die Datei `/etc/inet/secret/ipseckeys` ein, und aktivieren Sie anschließend den `svc:/network/ipsec/manual-key:default`-Service. Die Verfahrensweise ist unter „So erstellen Sie manuell IPsec-Sicherheitszuordnungen“ auf Seite 545 erläutert.

Obwohl der Befehl `ipseckey` nur über wenige allgemeine Optionen verfügt, unterstützt er eine umfangreiche Befehlssprache. Sie können festlegen, dass Anforderungen mittels einer programmatischen Schnittstelle zugestellt werden, die speziell für die manuelle Schlüsselerstellung gilt. Weitere Informationen finden Sie in der Manpage `pf_key(7P)`.

Sicherheitsbetrachtungen für `ipseckey`

Mit dem `ipseckey`-Befehl können Sie als Superuser oder in einer Rolle mit dem Rechteprofil für Netzwerksicherheit bzw. Netzwerk-IPsec-Management vertrauliche kryptografische Informationen eingeben. Wenn ein potenzieller Gegner Zugriff auf diese Informationen erhält, könnte er die Sicherheit des IPsec-Datenverkehrs beeinflussen.

Berücksichtigen Sie bei der Verwaltung des Schlüsselmaterials und dem Verwenden des Befehls `ipseckey` sollten Sie die folgenden Punkte:

- Haben Sie das Schlüsselmaterial aktualisiert? Eine regelmäßige Schlüsselaktualisierung ist eine grundlegende Sicherheitsanforderung. Die Schlüsselaktualisierung schützt gegen potentielle Schwächen von Algorithmen und Schlüsseln und verhindert größere Schäden durch einen offen liegenden Schlüssel.
- Verläuft das TTY über ein Netzwerk? Wird der Befehl `ipseckey` im interaktiven Modus ausgeführt?
  - Im interaktiven Modus ist die Sicherheit des Schlüsselmaterials die Sicherheit für den Netzwerkpfad dieses TTY-Verkehrs. Vermeiden Sie, den Befehl `ipseckey` über eine Reintext-Telnet- oder rlogin-Sitzung zu verwenden.
  - Auch lokale Fenster können von einem versteckten Programm angegriffen werden, das die Ereignisse im Fenster ausliest.
- Haben Sie die Option `-f` verwendet? Wird über das Netzwerk auf die Datei zugegriffen? Kann die Datei von Außenstehenden gelesen werden?
  - Ein potentieller Angreifer kann eine über das Netzwerk eingehängte Datei lesen, wenn die Datei eingelesen wird. Vermeiden Sie, für das Schlüsselmaterial eine für Außenstehende lesbare Datei zu verwenden.
  - Schützen Sie Ihr Benennungssystem. Wenn die folgenden beiden Bedingungen erfüllt sind, sind Ihre Hostnamen nicht mehr vertrauenswürdig:
    - Ihre Quelladresse ist ein Host, der über das Netzwerk nachgeschlagen werden kann.
    - Ihr Benennungssystem wurde kompromittiert.

Sicherheitsschwächen beruhen häufig auf dem Fehlverhalten von Tools, nicht von tatsächlichen Tools. Aus diesem Grund sollten Sie bei der Verwendung des `ipseckey`-Befehls vorsichtig sein. Verwenden Sie eine Konsole oder ein anderes festverdrahtetes TTY für den sichersten Betriebsmodus.

IPsec-Erweiterungen für andere Dienstprogramme

Der Befehl `ifconfig` verfügt über Optionen zur Verwaltung der IPsec-Richtlinie für eine Tunnelschnittstelle. Der Befehl `snoop` kann AH- und ESP-Header analysieren.

`ifconfig`-Befehl und IPsec

In den Releases Solaris 10, Solaris 10 7/05, Solaris 10 1/06 und Solaris 10 11/06: Zur Unterstützung von IPsec stehen die folgenden Sicherheitsoptionen über den Befehl `ifconfig` zur Verfügung. Diese Sicherheitsoptionen werden vom Befehl `ipsecconf` im Solaris 10 7/07-Release verarbeitet.

- auth_algs
- encr_auth_algs
- encr_algs

Sie müssen alle IPsec-Sicherheitsoptionen für einen Tunnel in einem Aufruf angeben. Angenommen, Sie verwenden zum Schützen des Verkehrs nur ESP, können Sie den Tunnel ip.tun0 einmal mit beiden Sicherheitsoptionen wie in dem folgenden Beispiel konfigurieren:

```
# ifconfig ip.tun0 encr_algs aes encr_auth_algs md5
```

Entsprechend wird ein ipsecinit.conf-Eintrag den Tunnel einmal mit beiden Sicherheitsoptionen konfigurieren. Betrachten Sie dazu das folgende Beispiel:

```
# WAN traffic uses ESP with AES and MD5.
   {} ipsec {encr_algs aes encr_auth_algs md5}
```

auth_algs-Sicherheitsoption

Diese Option aktiviert einen IPsec AH-Header mit einem bestimmten Authentifizierungsalgorithmus für einen Tunnel. Die Option auth_algs hat das folgende Format:

auth_algs *authentication-algorithm*

Als Algorithmus können Sie entweder eine Zahl oder einen Algorithmusnamen einschließlich dem Parameter *any* verwenden, so dass kein bestimmter Algorithmus bevorzugt wird. Zum Deaktivieren der Tunnelsicherheit geben Sie die folgende Option an:

```
auth_algs none
```

Zum Anzeigen einer Liste der verfügbaren Authentifizierungsalgorithmen geben Sie den Befehl ipsecalgs ein.

Hinweis – Die Option auth_algs arbeitet nicht mit NAT-Traversal. Weitere Informationen finden Sie unter „IPsec und NAT Traversal“ auf Seite 528.

---

encr_auth_algs-Sicherheitsoption

Diese Option aktiviert einen IPsec ESP-Header mit einem bestimmten Authentifizierungsalgorithmus für einen Tunnel. Die Option encr_auth_algs hat das folgende Format:

encr_auth_algs *authentication-algorithm*

Als Algorithmus können Sie entweder eine Zahl oder einen Algorithmusnamen einschließlich dem Parameter *any* verwenden, so dass kein bestimmter Algorithmus bevorzugt wird. Wenn

Sie einen ESP-Verschlüsselungsalgorithmus, aber keinen Authentifizierungsalgorithmus angeben, nimmt der Werte für den ESP-Authentifizierungsalgorithmus standardmäßig den Parameter *any* an.

Zum Anzeigen einer Liste der verfügbaren Authentifizierungsalgorithmen geben Sie den Befehl `ipsecalgs` ein.

`encr_algs`-Sicherheitsoption

Diese Option aktiviert einen IPsec ESP-Header mit einem bestimmten Verschlüsselungsalgorithmus für einen Tunnel. Die Option `encr_algs` hat das folgende Format:

`encr_algs` *encryption-algorithm*

Als Algorithmus können Sie entweder eine Zahl oder den Algorithmusnamen angeben. Zum Deaktivieren der Tunnelsicherheit geben Sie die folgende Option an:

```
encr_algs none
```

Wenn Sie einen ESP-Authentifizierungsalgorithmus, aber keinen Verschlüsselungsalgorithmus angeben, nimmt der Wert der ESP-Verschlüsselung standardmäßig den Parameter *null* an.

Zum Anzeigen einer Liste der verfügbaren Verschlüsselungsalgorithmen geben Sie den Befehl `ipsecalgs` ein.

`snoop`-Befehl und IPsec

Der Befehl `snoop` kann AH- und ESP-Header analysieren. Da ESP seine Daten verschlüsselt, sieht der Befehl `snoop` keine verschlüsselten Header, die durch ESP geschützt wurden. AH verschlüsselt keine Daten. Aus diesem Grund kann Datenverkehr, der durch AH geschützt wird, mit dem Befehl `snoop` geprüft werden. Die Befehlsoption `-V` zeigt, wann AH für ein Paket verwendet wird. Weitere Informationen finden Sie in der Manpage `snoop`(1M).

Ein Beispiel einer ausführlichen Ausgabe des Befehls `snoop` bei einem geschützten Paket finden Sie unter „So prüfen Sie, ob Pakete mit IPsec geschützt sind“ auf Seite 550.

Internet Key Exchange (Übersicht)

Internet Key Exchange (IKE) automatisiert das Schlüsselmanagement für IPsec. Dieses Kapitel enthält die folgenden Informationen zum IKE:

- „Neuerungen bei IKE“ auf Seite 603
- „Schlüsselmanagement mit IKE“ auf Seite 604
- „IKE-Schlüsselaushandlung“ auf Seite 604
- „IKE-Konfigurationsmöglichkeiten“ auf Seite 606
- „IKE und Hardwarebeschleunigung“ auf Seite 608
- „IKE und Hardware-Speicherung“ auf Seite 608
- „IKE-Dienstprogramme und Dateien“ auf Seite 608
- „Änderungen an IKE für das Release Solaris 10“ auf Seite 610

Anweisungen zur Implementierung von IKE finden Sie in Kapitel 23, „Konfiguration von IKE (Aufgaben)“. Referenzinformationen finden Sie in Kapitel 24, „Internet Key Exchange (Referenz)“. Referenzinformationen zu IPsec finden Sie in Kapitel 19, „IP Security Architecture (Übersicht)“.

Neuerungen bei IKE

Solaris 10 4/09: Ab dieser Version wird IKE in der Service Management Facility (SMF) als Service verwaltet. Standardmäßig ist der Service `svc:/network/ipsec/ike:default` deaktiviert. Ebenfalls in dieser Version wird das Rechteprofil für das Netzwerk-IPsec-Management (zur Verwaltung von IPsec und IKE) bereitgestellt.

Solaris 10 7/07: Ab diesem Release kann IKE den AES-Algorithmus benutzen und in der globalen Zone für die Verwendung in nicht-globalen Zonen konfiguriert werden.

- Mit der Socket-Option `SO_ALLZONES` kann IKE Datenverkehr in nicht-globalen Zonen verarbeitet werden.
- Eine vollständige Liste der neuen Funktionen in Solaris sowie eine Beschreibung der Solaris-Versionen finden Sie in *Neuerungen in Oracle Solaris 9 10/10*.

Schlüsselmanagement mit IKE

Die Verwaltung des Schlüsselmaterials für IPsec-Sicherheitszuordnungen (SAs) wird als *Schlüsselmanagement* bezeichnet. Für das automatische Schlüsselmanagement ist ein sicherer Kommunikationskanal erforderlich, damit Schlüsseln ordnungsgemäß erstellt, authentifiziert und ausgetauscht werden können. Das Solaris OS verwendet Internet Key Exchange (IKE) zum automatischen Schlüsselmanagement. IKE lässt sich mit einfachen Mitteln skalieren, um einen sicheren Kanal für hohen Datenverkehr bereitzustellen. IPsec SAs für IPv4- und IPv6-Pakete können von den Vorteilen von IKE profitieren.

Wird IKE auf einem System mit einem Sun Crypto Accelerator 1000-, einem Sun Crypto Accelerator 4000-oder einem Sun Crypto Accelerator 6000-Board betrieben, können die öffentlichen Schlüsselvorgänge an den Beschleuniger abgegeben werden. Die Betriebssystemressourcen werden dann nicht für PublicKey-Vorgänge genutzt. Wird IKE auf einem System mit einem Sun Crypto Accelerator 4000 oder einem Sun Crypto Accelerator 6000-Board verwendet, können die Zertifikate, Public Keys und Private Keys auf dem Board gespeichert werden. Die Schlüsselspeicherung findet außerhalb des Systems statt, um für eine zusätzliche Sicherheitsschicht zu sorgen.

IKE-Schlüsselaushandlung

Der IKE-Daemon `in.iked` sorgt für eine sichere Aushandlung und Authentifizierung des Schlüsselmaterials für SAs. Der Daemon verwendet Zufalls-Seeds für Schlüssel aus internen Funktionen, die von Solaris OS bereitgestellt werden. IKE bietet umfassende Sicherheit bei Weiterleitungen (PFS, Perfect Forward Secrecy). Bei PFS können die Schlüssel, mit denen die Datenübertragung geschützt wird, nicht zum Ableiten von weiteren Schlüsseln verwendet werden. Außerdem können Seeds, die zum Erstellen von Datenübertragungsschlüsseln verwendet werden, nicht wieder verwendet werden. Weitere Informationen finden Sie in der Manpage `in.iked`(1M).

Wenn der IKE-Daemon einen öffentlichen Chiffrierschlüssel eines Remote-Systems erfasst, kann das lokale System diesen Schlüssel verwenden. Das System verschlüsselt Nachrichten mithilfe des öffentlichen Schlüssels des Remote-Systems. Die Nachrichten können nur von diesem Remote-System gelesen werden. Der IKE-Daemon arbeitet in zwei Stufen. Diese Stufen werden als *exchanges* (Austauschvorgänge) bezeichnet.

IKE-Schlüssel – Terminologie

In der folgenden Tabelle sind Begriffe aufgeführt, die bei der Schlüsselaushandlung verwendet werden. Darüber hinaus sind Akronyme, Erklärungen und Verwendungsmöglichkeiten für jeden Begriff angegeben.

TABELLE 22–1 Begriffe, Akronyme und Verwendungsmöglichkeiten bei der Schlüsselaushandlung

Begriff	Acronym	Definition und Verwendung
Key Exchange		Der Prozess zum Erzeugen von Schlüsseln für asymmetrische kryptografische Algorithmen. Die zwei wichtigsten Methoden sind die RSA-Protokolle und das Diffie-Hellman-Protokoll.
Diffie-Hellman-Protokoll	DH	Ein Key Exchange-Protokoll zur Erzeugung und Authentifizierung von Schlüsseln. Wird häufig auch als *authentifizierter Schlüsselaustausch* bezeichnet.
RSA-Protokoll	RSA	Ein Key Exchange-Protokoll zur Erzeugung und Verteilung von Schlüsseln. Das Protokoll ist nach seinen drei Autoren Rivest, Shamir und Adleman benannt.
Perfect Forward Secrecy	PFS	Gilt nur für authentifizierten Schlüsselaustausch. PFS stellt sicher, dass sich langfristig sicheres Schlüsselmaterial nicht negativ auf die Geheimhaltung von Schlüsseln auswirkt, die bei früheren Kommunikationen ausgetauscht wurden. Bei PFS kann der Schlüssel, der zum Schützen der Datenübertragung verwendet wird, nicht zum Ableiten weiterer Schlüssel verwendet werden. Außerdem wird die Quelle des Schlüssels, der zum Schützen von Datenübertragungen verwendet wird, niemals zum Ableiten weiterer Schlüssel verwendet.
Oakley-Methode		Eine Methode zum sicheren Erstellen der Schlüssel für Stufe 2. Das Protokoll ist analog zur Diffie-Hellman-Methode beim Key Exchange. Wie Diffie-Hellman führt der Schlüsselaustausch der Oakley-Methode Schlüsselerzeugung und Schlüsselauthentifizierung aus. Die Oakley-Methode dient zur Aushandlung von PFS.

IKE Phase 1 Exchange

Der Phase 1 Exchange wird als *Hauptmodus* bezeichnet. Im Phase 1 Exchange verwendet IKE Verschlüsselungsmethoden mit öffentlichem Schlüssel, um sich selbst gegenüber IKE-Peer-Entitäten zu authentifizieren. Das Ergebnis ist eine Internet Security Association and Key Management Protocol (ISAKMP)-Sicherheitszuordnung (SA). Eine ISAKMP SA ist ein sicherer Kanal für IKE zur Aushandlung des Schlüsselmaterials für IP-Datagramme. Im Gegensatz zu IPsec SAs sind ISAKMP SAs bidirektional, daher wird nur eine Sicherheitszuordnung benötigt.

Das Verfahren zur Aushandlung des Schlüsselmaterials durch IKE beim Phase 1 Exchange kann konfiguriert werden. IKE liest die Konfigurationsinformationen in der Datei `/etc/inet/ike/config` ein. Die Konfigurationsinformationen umfassen Folgendes:

- Globale Parameter, z. B. die Namen der öffentlichen Schlüsselzertifikate
- Ob Perfect Forward Secrecy (PFS) verwendet wird
- Die betroffenen Schnittstellen

- Die Sicherheitsprotokolle und deren Algorithmen
- Die Authentifizierungsmethode

Die zwei Authentifizierungsmethoden sind PresharedKeys und PublicKey-Zertifikate. Die PublicKey-Zertifikate können selbst-signiert sein. Die Zertifikate können auch von einer Zertifizierungsstelle (Certificate authority, CA), einer PublicKey-Infrastruktur (PKI)-Organisation ausgegeben werden. Diese Organisationen sind z. B. beTrusted, Entrust, GeoTrust, RSA Security und Verisign.

IKE Phase 2 Exchange

Der Phase 2 Exchange wird als *Schnellmodus* bezeichnet. Beim Phase 2 Exchange erstellt und verwaltet IKE die IPsec SAs zwischen Systemen, die den IKE-Daemon ausführen. IKE verwendet den sicheren Kanal, der in Phase 1 erstellt wurde, für den Schutz der Übertragung des Schlüsselmaterials. Der IKE-Daemon erstellt die Schlüssel mithilfe des Geräts `/dev/random` aus einem Zufallszahlengenerator. Der Daemon aktualisiert die Schlüssel in einem konfigurierbaren Intervall. Das Schlüsselmaterial steht Algorithmen zur Verfügung, die in der Konfigurationsdatei für die IPsec-Richtlinie, `ipsecinit.conf`, angegeben sind.

IKE-Konfigurationsmöglichkeiten

Die Konfigurationsdatei `/etc/inet/ike/config` enthält Einträge für die IKE-Richtlinie. Damit zwei IKE-Daemons einander authentifizieren, müssen die Einträge gültig sein und das Schlüsselmaterial muss zur Verfügung stehen. Die Einträge in der Konfigurationsdatei bestimmen die Methode, in der das Schlüsselmaterial zur Authentifizierung des Phase 1 Exchange verwendet wird. Die Auswahlmöglichkeiten sind PresharedKeys oder PublicKey-Zertifikate.

Der Eintrag `auth_method preshared` legt fest, dass PresharedKeys verwendet werden. Andere Werte als `preshared` für `auth_method` kennzeichnen, dass PublicKey-Zertifikate verwendet werden. PublicKey-Zertifikate können selbst-signiert sein oder die Zertifikate können von einer PKI-Organisation installiert werden. Weitere Informationen finden Sie in der Manpage `ike.config`(4).

IKE mit PresharedKeys

PresharedKeys werden von einem Administrator auf einem System erstellt. Die Schlüssel werden dann außerbandig an die Administratoren der remoten Systeme weitergegeben. Achten Sie darauf, umfangreiche Zufallsschlüssel zu erzeugen und die Datei sowie die außerbandige Übertragung zu schützen. Die Schlüssel werden auf jedem System in der Datei `/etc/inet/secret/ike.preshared` abgelegt. Die Datei `ike.preshared` gilt für IKE , die Datei `ipseckeys` für IPsec. Eine Sicherheitsgefährdung der Schlüssel in der Datei `ike.preshared` gefährdet alle Schlüssel, die von den Schlüsseln in dieser Datei abgeleitet sind.

Ein Preshared-Schlüssel eines Systems muss identisch mit dem Schlüssel seines remoten Systems sein. Die Schlüssel sind an eine bestimmte IP-Adresse gebunden. Die Schlüssel sind am sichersten, wenn ein Administrator die kommunizierenden Systeme verwaltet. Weitere Informationen finden Sie in der Manpage `ike.preshared(4)`.

IKE mit PublicKey-Zertifikaten

Mit PublicKey-Zertifikaten müssen kommunizierende Systeme kein geheimes außerbandiges Schlüsselmaterial mehr verwenden. PublicKeys verwenden das Diffie-Hellman-Protokoll (DH) zur Authentifizierung und Aushandlung von Schlüsseln. PublicKey-Zertifikate gibt es in zwei Ausführungen. Die Zertifikate können selbst-signiert sein, oder sie werden von einer Zertifizierungsstelle (Certificate authority, CA) zertifiziert.

Selbst-signierte PublicKey-Zertifikate werden von Ihnen, dem Administrator, erstellt. Mit dem Befehl `ikecert certlocal -ks` erstellen Sie den privaten Teil eines PublicKey-PrivateKey-Paars für das System. Dann erhalten Sie die selbst-signierte Zertifikatsausgabe im X.509-Format vom remoten System. Das Zertifikat des remoten Systems wird als öffentlicher Teil des Key-Paars in den Befehl `ikecert certdb` eingegeben. Die selbst-resignierten Zertifikate befinden sich in dem Verzeichnis `/etc/inet/ike/publickeys` der kommunizierenden Systeme. Wenn Sie die Option `-T` verwenden, befinden sich die Zertifikate auf einer angehängten Hardware.

Selbst-designierte Zertifikate stellen einen Kompromiss zwischen PresharedKeys und CAs dar. Im Gegensatz zu PresharedKeys kann ein selbst-signiertes Zertifikat auf einem mobilen Computer oder auf einem System verwendet werden, das neu nummeriert werden kann. Um ein Zertifikat für ein System ohne feststehende Nummer selbst zu signieren, verwenden Sie einen alternativen `DNS`-Namen (`www.example.org`) oder `email` (`root@domain.org`).

PublicKeys können von einer PK- oder einer CA-Organisation erstellt werden. Sie installieren die PublicKeys und deren begleitenden CAs im Verzeichnis `/etc/inet/ike/publickeys.` Wenn Sie die Option `-T` verwenden, befinden sich die Zertifikate auf einer angehängten Hardware. Anbieter veröffentlichen auch Listen der zurückgenommenen Zertifikate (Certificate Revocation-Lists, CRLs). Neben den Schlüsseln und CAs müssen Sie als Administrator auch die CRL im Verzeichnis `/etc/inet/ike/crls` installieren.

CAs haben den Vorteil, dass sie von einer außenstehenden Organisation und nicht vom Standort-Administrator zertifiziert werden. In gewisser Hinsicht sind CAs notariell beglaubigte Zertifikate. Wie auch selbst-signierte Zertifikate können CAs auf einem mobilen Computer oder auf einem System verwendet werden, dass neu nummeriert werden kann. Im Gegensatz zu selbst-signierten Zertifikaten können CAs leicht skaliert werden, um zahlreiche miteinander kommunizierende Systeme zu schützen.

IKE und Hardwarebeschleunigung

IKE-Algorithmen erfordern umfangreiche Berechnungen, insbesondere beim Phase 1 Exchange. Systeme, die zahlreiche Austauschvorgänge verarbeiten müssen, sollten ein Sun Crypto Accelerator 1000-Board zur Verarbeitung der PublicKey-Vorgänge verwenden. Die Sun Crypto Accelerator 6000- und Sun Crypto Accelerator 4000-Boards können auch für teuere Phase 1-Berechnungen verwendet werden.

Weitere Informationen, wie Sie IKE zum Ausführen der Berechnungen auf dem Beschleunigerboard konfigurieren, finden Sie unter „So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 1000-Board“ auf Seite 651. Informationen zum Speichern von Schlüsseln finden Sie unter„So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 4000-Board“ auf Seite 652 und in der Manpage `cryptoadm(1M)`.

IKE und Hardware-Speicherung

Public Key-Zertifikate, Private Keys und Public Keys können auf einem Sun Crypto Accelerator 6000- oder einem Sun Crypto Accelerator 4000-Board gespeichert werden. Bei der RSA-Verschlüsselung unterstützt das Sun Crypto Accelerator 4000-Board Schlüssel bis zu einer Länge von 2048 Bit. Bei der DSA-Verschlüsselung unterstützt das Board Schlüssel bis zu einer Länge von 1024 Bit. Das Sun Crypto Accelerator 6000-Board unterstützt die SHA-512- und ECC-Algorithmen.

Informationen zur Konfiguration von IKE für den Zugriff auf das Board finden Sie unter „So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 1000-Board“ auf Seite 651. Informationen zum Hinzufügen von Zertifikaten und PublicKeys zum Board finden Sie unter „So erzeugen Sie PublicKey-Zertifikate und speichern sie auf angehängter Hardware“ auf Seite 636.

IKE-Dienstprogramme und Dateien

In der folgenden Tabelle sind die Konfigurationsdateien für die IKE-Richtlinie, die Speicherorte für IKE-Schlüssel und die verschiedenen IKE-Befehle und -Services zusammengefasst. Weitere Informationen zu Services finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration*.

TABELLE 22–2 IKE-Konfigurationsdateien, Speicherorte für Schlüssel, Befehle und Services

Datei, Speicherort, Befehl oder Service	Beschreibung	Weitere Informationen
`svc:/network/ipsec/ike`	Der SMF-Service, der in der aktuellen Version die IKE-Verwaltung übernimmt.	`smf(5)`

TABELLE 22–2 IKE-Konfigurationsdateien, Speicherorte für Schlüssel, Befehle und Services *(Fortsetzung)*

Datei, Speicherort, Befehl oder Service	Beschreibung	Weitere Informationen
`/usr/lib/inet/in.iked`-Daemon	Internet Key Exchange (IKE)-Daemon. Aktiviert die automatisierte Schlüsselverwaltung. In der aktuellen Version wird dieser Daemon durch den `ike`-Service aktiviert. In älteren Versionen wird der `in.iked`-Befehl verwendet.	`in.iked`(1M)
`/usr/sbin/ikeadm`-Befehl	IKE-Verwaltungsbefehl zum Anzeigen und Ändern der IKE-Richtlinie.	`ikeadm`(1M)
`/usr/sbin/ikecert`-Befehl	Befehl zur Verwaltung der Zertifikatdatenbank, mit dem lokale Datenbanken geändert werden können, die PublicKey-Zertifikate enthalten. Die Datenbanken können auch auf einem angehängtem Sun Crypto Accelerator 4000-Board gespeichert werden.	`ikecert`(1M)
`/etc/inet/ike/config`-Datei	Standardkonfigurationsdatei für die IKE-Richtlinie im Verzeichnis `/etc/inet`. Enthält die Regeln des Standorts für passende eingehende IKE-Anforderungen und zur Vorbereitung von abgehenden IKE-Anforderungen. Falls diese Datei vorhanden ist, wird in der aktuellen Version der `in.iked`-Daemon gestartet, sobald der `ike`-Service aktiviert wird. Der Speicherort dieser Datei kann über den Befehl `svccfg` geändert werden.	`ike.config`(4)
`ike.preshared`-Datei	PresharedKeys-Datei im Verzeichnis `/etc/inet/secret`. Enthält sicheres Schlüsselmaterial für die Authentifizierung im Phase 1 Exchange. Wird bei der Konfiguration von IKE mit PresharedKeys verwendet.	`ike.preshared`(4)
`ike.privatekeys`-Verzeichnis	PrivateKeys-Verzeichnis im Verzeichnis `/etc/inet/secret`. Enthält die privaten Schlüssel, die Teil eines PublicKey-PrivateKey-Paares sind.	`ikecert`(1M)
`publickeys`-Verzeichnis	Verzeichnis im `/etc/inet/ike`-Verzeichnis, in dem PublicKeys und Zertifikatsdateien gespeichert sind. Enthält die öffentlichen Schlüssel, die Teil eines PublicKey-PrivateKey-Paares sind.	`ikecert`(1M)
`crls`-Verzeichnis	Verzeichnis im `/etc/inet/ike`-Verzeichnis, in dem Widerrufslisten (CRLs) für PublicKeys und Zertifikatsdateien gespeichert sind.	`ikecert`(1M)
Sun Crypto Accelerator 1000-Board	Hardware, mit der PublicKey-Vorgänge beschleunigt werden, indem die Berechnung dieser Vorgänge für das Betriebssystem übernommen werden.	`ikecert`(1M)

TABELLE 22–2 IKE-Konfigurationsdateien, Speicherorte für Schlüssel, Befehle und Services *(Fortsetzung)*

Datei, Speicherort, Befehl oder Service	Beschreibung	Weitere Informationen
Sun Crypto Accelerator 4000-Board	Hardware, mit der PublicKey-Vorgänge beschleunigt werden, indem die Berechnung dieser Vorgänge für das Betriebssystem übernommen werden. Außerdem können PublicKeys, PrivateKeys und PublicKey-Zertifikate auf dem Board gespeichert werden.	`ikecert(1M)`

Änderungen an IKE für das Release Solaris 10

Nach dem Release Solaris 9 wurde IKE um die folgenden Leistungsmerkmale erweitert:

- IKE kann zur Automatisierung des Schlüsselaustauschs für IPsec über IPv6-Netzwerke verwendet werden. Weitere Informationen finden Sie unter „Schlüsselmanagement mit IKE“ auf Seite 604.

Hinweis – IKE kann nicht zur Verwaltung von Schlüsseln für IPsec in einer nicht-globalen Zone verwendet werden.

- PublicKey-Vorgänge in IKE können mithilfe eines Sun Crypto Accelerator 1000-Boards oder eines Sun Crypto Accelerator 4000-Boards beschleunigt werden. Die Berechnungen der Vorgänge können vom Board übernommen werden. Durch die Entlastung der CPU wird die Verschlüsselung beschleunigt und somit der Bedarf an Betriebssystemressourcen reduziert. Weitere Informationen finden Sie unter „IKE und Hardwarebeschleunigung“ auf Seite 608. Anweisungen finden Sie unter „Konfiguration von IKE zum Suchen angehängter Hardware (Übersicht der Schritte)“ auf Seite 650.
- PublicKey-Zertifikate, PrivateKeys und PublicKeys können auf einem Sun Crypto Accelerator 4000-Board gespeichert werden. Weitere Informationen zur Schlüsselspeicherung finden Sie unter „IKE und Hardware-Speicherung“ auf Seite 608.
- IKE kann zur Automatisierung des Schlüsselaustauschs für IPsec hinter einer NAT-Box verwendet werden. Der Datenverkehr muss ein IPv4-Netzwerk nutzen. Außerdem können NAT-durchlaufende IPsec ESP-Schlüssel nicht Hardware-beschleunigt werden. Weitere Informationen finden Sie unter „IPsec und NAT Traversal“ auf Seite 528. Anweisungen finden Sie unter „Konfiguration von IKE für mobile Systeme (Übersicht der Schritte)“ auf Seite 642.
- Der Datei `/etc/inet/ike/config` wurden Parameter zur erneuten Übertragung und zur Paket-Zeitüberschreitung hinzugefügt. Diese Parameter optimieren die Aushandlung in der IKE Phase 1 (Hauptmodus) zur Verarbeitung von Netzwerkstörungen, starkem Netzwerkverkehr und zur Interoperation mit Plattformen, die andere Implementierungen des IKE-Protokolls verwenden. Einzelheiten zu den Parametern finden Sie in der Manpage `ike.config(4)` Anweisungen finden Sie unter „Ändern der IKE-Übertragungsparameter (Übersicht der Schritte)“ auf Seite 654.

KAPITEL 23

Konfiguration von IKE (Aufgaben)

In diesem Kapitel wird beschrieben, wie Sie den Internet Key Exchange (IKE) für Ihre Systeme konfigurieren. Nachdem IKE konfiguriert wurde, erzeugt es automatisch das für die Ausführung von IPsec in Ihrem Netzwerk erforderliche Schlüsselmaterial. Dieses Kapitel enthält die folgenden Informationen:

- „Konfiguration von IKE (Übersicht der Schritte)" auf Seite 611
- „Konfiguration von IKE mit PresharedKeys (Übersicht der Schritte)" auf Seite 612
- „Konfiguration von IKE mit PublicKey-Zertifikaten (Übersicht der Schritte)" auf Seite 624
- „Konfiguration von IKE für mobile Systeme (Übersicht der Schritte)" auf Seite 642
- „Konfiguration von IKE zum Suchen angehängter Hardware (Übersicht der Schritte)" auf Seite 650
- „Ändern der IKE-Übertragungsparameter (Übersicht der Schritte)" auf Seite 654

Eine Einführung in IKE finden Sie in Kapitel 22, „Internet Key Exchange (Übersicht)". Referenzinformationen zu IKE finden Sie in Kapitel 24, „Internet Key Exchange (Referenz)". Weitere Verfahren finden Sie im Beispielbereich der Manpages `ikeadm`(1M), `ikecert`(1M) und `ike.config`(4).

Konfiguration von IKE (Übersicht der Schritte)

Zur Authentifizierung von IKE können Sie PresharedKeys, selbst-designierte Zertifikate und Zertifikate von einer Zertifizierungsstelle (Certificate Authority, CA) verwenden. Eine Regel verbindet die jeweilige IKE-Authentifizierungsmethode mit den zu schützenden Endpunkten. Aus diesem Grund können Sie eine oder alle IKE-Authentifizierungsmethoden in einem System verwenden. Mit einem Zeiger auf die PKCS&;#11-Bibliothek können Zertifikate auch einen angehängten Hardwarebeschleuniger verwenden.

Nachdem Sie IKE konfiguriert haben, führen Sie die IPsec-Aufgabe aus, in der die IKE-Konfiguration verwendet wird. In der folgenden Tabelle wird auf die Übersichten verwiesen, die sich auf eine bestimmte IKE-Konfiguration beziehen.

Aufgabe	Beschreibung	Siehe
Konfiguration von IKE mit PresharedKeys	Schützen Sie die Kommunikation zwischen zwei Systemen, in dem die Systeme einen geheimen Schlüssel gemeinsam nutzen.	„Konfiguration von IKE mit PresharedKeys (Übersicht der Schritte)“ auf Seite 612
Konfiguration von IKE mit PublicKey-Zertifikaten	Schützen Sie die Kommunikation mit PublicKey-Zertifikaten. Die Zertifikate können selbst-signiert oder von einer PKI-Organisation ausgestellt worden sein.	„Konfiguration von IKE mit PublicKey-Zertifikaten (Übersicht der Schritte)“ auf Seite 624
Durchlaufen einer NAT-Grenze	Konfigurieren Sie IPsec und IKE zur Kommunikation mit einem mobilen System.	„Konfiguration von IKE für mobile Systeme (Übersicht der Schritte)“ auf Seite 642
Konfiguration von IKE zum Erzeugen und Speichern von PublicKey-Zertifikaten auf angehängter Hardware	Setzen Sie ein Sun Crypto Accelerator 1000-Board oder ein Sun Crypto Accelerator 4000-Board ein, um die Berechnung von IKE-Vorgängen zu beschleunigen. Auf dem Sun Crypto Accelerator 4000-Board können auch die PublicKey-Zertifikate gespeichert werden.	„Konfiguration von IKE zum Suchen angehängter Hardware (Übersicht der Schritte)“ auf Seite 650
Optimieren der Phase 1-Parameter zur Schlüsselaushandlung	Ändern Sie den Zeitpunkt der IKE-Schlüsselaushandlungen.	„Ändern der IKE-Übertragungsparameter (Übersicht der Schritte)“ auf Seite 654

Konfiguration von IKE mit PresharedKeys (Übersicht der Schritte)

In der folgenden Tabelle wird auf Verfahren zur Konfiguration und Verwaltung von IKE mit PresharedKeys verwiesen.

Aufgabe	Beschreibung	Siehe
Konfiguration von IKE mit PresharedKeys	Erstellen Sie eine IKE-Richtliniendatei und einen gemeinsam zu nutzenden Schlüssel.	„So konfigurieren Sie IKE mit PresharedKeys“ auf Seite 613
Aktualisieren der PresharedKeys auf einem laufenden IKE-System	Fügen Sie neues Schlüsselmaterial für IKE auf den kommunizierenden Systemen hinzu.	„So werden IKE PresharedKeys aktualisiert“ auf Seite 616
Hinzufügen von PresharedKeys zu einem laufenden IKE-System	Fügen Sie einen neuen IKE-Richtlinieneintrag und neues Schlüsselmaterial zu einem System hinzu, das derzeit eine IKE-Richtlinie durchsetzt.	„So fügen Sie einen IKE PresharedKey für einen neuen Richtlinieneintrag in `ipsecinit.conf` ein“ auf Seite 619
Prüfen, ob die PresharedKeys identisch sind	Zeigen Sie die PresharedKeys auf beiden Systemen an, so dass Sie feststellen können, ob die Schlüssel identisch sind	„So prüfen Sie, ob die IKE PresharedKeys identisch sind“ auf Seite 622

Konfiguration von IKE mit PresharedKeys

PresharedKeys ist die einfachste Authentifizierungsmethode für IKE. Wenn Sie beide Systeme so könfigurieren, dass sie IKE verwenden und Administrator beide Systeme sind, ist die Methode PresharedKeys eine gute Wahl. Im Gegensatz zu PublicKey-Zertifikaten sind PresharedKeys jedoch an bestimmte IP-Adressen gebunden. PresharedKeys können daher nicht mit mobilen Systemen oder Systemen verwendet werden, die neue Adressen erhalten. Darüber hinaus können Sie bei der Verwendung von PresharedKeys die Berechnung von IKE-Vorgängen nicht an angehängte Hardware abgeben.

▼ So konfigurieren Sie IKE mit PresharedKeys

Die IKE-Implementierung bietet Algorithmen, deren Schlüssel unterschiedlich lang sind. Die von Ihnen gewählte Schlüssellänge wird von der Standortsicherheit vorgegeben. Im Allgemeinen bieten längere Schlüssel größere Sicherheit als kürzere Schlüssel.

In diesen Verfahren werden die Systeme `enigma` und `partym` verwendet. Ersetzen Sie `enigma` und `partym` durch die Namen Ihrer Systeme.

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

   Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

   ---

2. **Kopieren Sie auf jedem System die Datei** `/etc/inet/ike/config.sample` **nach** `/etc/inet/ike/config`**.**

3 Geben Sie die Regeln und globalen Parameter auf jedem System in die Datei `ike/config` ein.

Die Regeln und globalen Parameter in dieser Datei müssen zulassen, dass die IPsec-Richtlinie in der Datei `ipsecinit.conf` auf dem System erfolgreich ist. Die folgenden `ike/config`-Beispiele arbeiten mit den `ipsecinit.conf`-Beispielen unter „So sichern Sie Datenverkehr zwischen zwei Systemen mit IPsec“ auf Seite 535.

a. Ändern Sie beispielsweise die Datei `/etc/inet/ike/config` auf dem System `enigma`:

```
### ike/config file on enigma, 192.168.116.16

## Global parameters
#
## Phase 1 transform defaults
p1_lifetime_secs 14400
p1_nonce_len 40
#
## Defaults that individual rules can override.
p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 2
#
## The rule to communicate with partym
#  Label must be unique
{ label "enigma-partym"
  local_addr 192.168.116.16
  remote_addr 192.168.13.213
  p1_xform
   { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
  p2_pfs 5
}
```

Hinweis – Alle Argumente für den Parameter `auth_method` müssen sich auf der gleichen Zeile befinden.

---

b. Ändern Sie die Datei `/etc/inet/ike/config` auf dem System `partym`:

```
### ike/config file on partym, 192.168.13.213
## Global Parameters
#
p1_lifetime_secs 14400
p1_nonce_len 40
#
p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 2

## The rule to communicate with enigma
#  Label must be unique
{ label "partym-enigma"
  local_addr 192.168.13.213
  remote_addr 192.168.116.16
p1_xform
   { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
p2_pfs 5
}
```

4 Prüfen Sie auf den einzelnen Systemen die Dateisyntax.

```
# /usr/lib/inet/in.iked -c -f /etc/inet/ike/config
```

5 Erzeugen Sie Zufallszahlen für das Schlüsselmaterial.

Falls Ihr Standort über einen Generator für Zufallszahlen verfügt, verwenden Sie diesen. Auf einem Solaris-System können Sie den Befehl od verwenden. Beispielsweise druckt der folgende Befehl zwei Zeilen mit hexadezimalen Zahlen:

```
% od -X -A n /dev/random | head -2
         f47cb0f4 32e14480 951095f8 2b735ba8
         0a9467d0 8f92c880 68b6a40e 0efe067d
```

Eine Beschreibung des Befehls od finden Sie unter „So erzeugen Sie Zufallszahlen auf einem Solaris-System“ auf Seite 543 und in der Manpage od(1).

Hinweis – Andere Betriebssysteme erfordern Schlüsselmaterial im ASCII-Format. Wie Sie einen identischen Schlüssel im hexadezimalen und im ASCII-Format erzeugen, finden Sie unter Beispiel 23–1.

---

6 Erzeugen Sie einen Schlüssel aus der Ausgabe in Schritt 5.

```
f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
```

Der Authentifizierungsalgorithmus in diesem Verfahren ist SHA–1 (wie in Schritt 3 gezeigt). Die Größe des Hash (d. h., die Größe der Ausgabe des Authentifizierungsalgorithmus) schreibt die empfohlene Mindestmenge für einen PresharedKey vor. Die Ausgabe des SHA–1-Algorithmus beträgt 160 Bit oder 40 Zeichen. Der Beispielschlüssel ist 56 Zeichen lang, wodurch IKE zusätzliches Schlüsselmaterial verwenden kann.

7 Erstellen Sie auf jedem System eine `/etc/inet/secret/ike.preshared`-Datei.

Geben Sie den PresharedKey in jede Datei ein.

a. Auf dem System `enigma` enthält die `ike.preshared`-Datei dann Folgendes:

```
# ike.preshared on enigma, 192.168.116.16
#...
{ localidtype IP
    localid 192.168.116.16
    remoteidtype IP
    remoteid 192.168.13.213
    # enigma and partym's shared key in hex (192 bits)
    key f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
    }
```

b. Auf dem System `partym` enthält die `ike.preshared`-Datei dann Folgendes:

```
# ike.preshared on partym, 192.168.13.213
#...
{ localidtype IP
    localid 192.168.13.213
    remoteidtype IP
```

```
        remoteid 192.168.116.16
        # partym and enigma’s shared key in hex (192 bits)
        key f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
        }
```

Hinweis – Die PresharedKeys auf den Systemen müssen identisch sein.

Beispiel 23–1 Erzeugen von identischem Schlüsselmaterial für zwei Systeme mit unterschiedlichen Betriebssystemen

Solaris IPsec kann mit anderen Betriebssystemen zusammenarbeiten. Falls Ihr System mit einem System kommuniziert, das PresharedKeys im ASCII-Format benötigt, müssen Sie einen Schlüssel in zwei Formaten, hexadezimal und ASCII, erstellen.

Im folgenden Beispiel möchte der Solaris-Systemadministrator 56 Zeichen für das Schlüsselmaterial verwenden. Der Administrator verwendet den folgenden Befehl, um einen hexadezimalen Schlüssel aus einem ASCII-Passwortsatz zu erzeugen. Mit der Option `-tx1` werden die Byte nacheinander auf allen Solaris-Systemen gedruckt.

```
# /bin/echo "papiermache with cashews and\c" | od -tx1 | cut -c 8-55 | \
tr -d ’\n’ | tr -d ’ ’ | awk ’{print}’
7061706965726d616368652077697468206361736865777320616e64
```

Durch Entfernen der Offsets und Verketten der hexadezimalen Ausgabe wird der hexadezimalen Schlüssel für das Solaris-System erstellt: `7061706965726d616368652077697468206361736865777320616e64`. Der Administrator fügt diesen Wert in die Datei `ike.preshared` auf dem Solaris-System ein.

```
# Shared key in hex (192 bits)
key 7061706965726d616368652077697468206361736865777320616e64
```

Auf dem System, das PresharedKeys im ASCII-Format erfordert, bildet der Passwortsatz den PresharedKey. Der Solaris-Systemadministrator sendet dem anderen Administrator telefonisch den Passwortsatz `papiermache with cashews and`.

▼ So werden IKE PresharedKeys aktualisiert

Bei diesem Verfahren wird davon ausgegangen, dass Sie einen vorhandenen PresharedKey in regelmäßigen Intervallen ersetzen möchten.

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

---

2 Erzeugen Sie Zufallszahlen und konstruieren Sie einen Schlüssel in der erforderlichen Länge.

Ausführliche Informationen finden Sie im Abschnitt „So erzeugen Sie Zufallszahlen auf einem Solaris-System“ auf Seite 543. Informationen zum Erzeugen von Schlüsselmaterial für ein Solaris-System, das mit einem Betriebssystem kommuniziert, das Schlüsselmaterial im ASCII-Format benötigt, finden Sie in Beispiel 23–1.

3 Ersetzen Sie den aktuellen Schlüssel durch einen neuen Schlüssel.

Bei den Hosts `enigma` und `partym` ersetzen Sie den Wert von `key` in der Datei `/etc/inet/secret/ike.preshared` durch eine Zahl der gleichen Länge.

4 Lesen Sie den neuen Schlüssel in den Systemkern ein.

- **Wenn Sie mindestens mit Solaris 10 4/09 arbeiten, aktualisieren Sie den `ike`-Service.**

```
# svcadm refresh ike
```

- **Wenn Sie eine ältere Version als Solaris 10 4/09 verwenden, muss der `in.iked`-Daemon beendet und neu gestartet werden.**

  a. Überprüfen Sie die Privilegstufe des `in.iked`-Daemons.

```
# /usr/sbin/ikeadm get priv
Current privilege level is 0x0, base privileges enabled
```

  Sie können das Schlüsselmaterial ändern, wenn dieser Befehl eine Privilegstufe von `0x1` oder `0x2` zurückgibt. Bei der Privilegstufe `0x0` ist das Ändern oder Anzeigen von Schlüsselmaterial nicht gestattet. Standardmäßig wird der `in.iked`-Daemon mit der Privilegstufe `0x0` ausgeführt.

  b. Lautet die Privilegstufe `0x0`, brechen Sie den Daemon ab und starten ihn neu.

  Wenn der Daemon neu startet, liest er die neue Version der `ike.preshared`-Datei ein.

```
# pkill in.iked
# /usr/lib/inet/in.iked
```

  c. Lautet die Privilegstufe `0x1` oder `0x2`, lesen Sie die neue Version der `ike.predshared`-Datei ein.

```
# ikeadm read preshared
```

▼ So rufen Sie IKE PresharedKeys auf

Standardmäßig verhindert der Befehl `ikeadm` die Anzeige der tatsächlichen Schlüssel in einem Speicherauszug einer Phase-1-SA. Die Anzeige der Schlüssel ist bei der Fehlersuche hilfreich.

Um die tatsächlichen Schlüssel anzuzeigen, müssen Sie die Privilegstufe für diesen Daemon erhöhen. Eine Beschreibung der Privilegstufe finden Sie unter „IKE-Verwaltungsbefehl“ auf Seite 659.

Hinweis – Wenn Sie dieses Verfahren in einer Version vor Solaris 10 4/09 durchführen möchten, schauen Sie sich die Hinweise unter Beispiel 23–2 an.

Bevor Sie beginnen IKE ist konfiguriert, und der `ike`-Service wird ausgeführt.

1. **Rufen Sie die IKE PresharedKeys auf.**

```
# ikeadm
ikeadm> dump preshared
```

2. **Wenn ein Fehler auftritt, erhöhen Sie die Privilegstufe des `in.iked`-Daemons.**

   a. **Erhöhen Sie die Privilegstufe des `in.iked`-Daemons im SMF-Repository.**

```
# svcprop -p config/admin_privilege ike
base
# svccfg -s ike setprop config/admin_privilege=keymat
```

   b. **Erhöhen Sie die Privilegstufe des ausgeführten `in.iked`-Daemons.**

```
# svcadm refresh ike ; svcadm restart ike
```

   c. **(Optional) Überprüfen Sie, ob die Privilegstufe `keymat` lautet.**

```
# svcprop -p config/admin_privilege ike
keymat
```

   d. **Zeigen Sie die Schlüssel an, indem Sie Schritt 1 erneut ausführen.**

3. **Legen Sie für den IKE-Daemon wieder die Basis-Privilegstufe fest.**

   a. **Legen Sie nach der Betrachtung der Schlüssel wieder die ursprüngliche Privilegstufe fest.**

```
# svccfg -s ike setprop config/admin_privilege=base
```

   b. **Aktualisieren Sie die Ansicht, und starten Sie IKE anschließend neu.**

```
# svcadm refresh ike ; svcadm restart ike
```

Beispiel 23–2 Überprüfen von IKE PresharedKeys in einer Version vor Solaris 10 4/09

Im folgenden Beispiel betrachtet der Administrator Schlüssel auf einem System mit einer älteren Solaris-Version. Der Administrator möchte sich vergewissern, dass die Schlüssel im System identisch mit den Schlüsseln im Kommunikationssystem sind. Nachdem der Administrator festgestellt hat, dass die Schlüssel der beiden Systeme identisch sind, stellt er die Privilegstufe 0 wieder her.

- Zuerst bestimmt der Administrator die Privilegstufe des `in.iked`-Daemons.

```
adm1 # /usr/sbin/ikeadm get priv
Current privilege level is 0x0, base privileges enabled
```

- Da die Privilegstufe nicht 0x1 bzw. 0x2 lautet, hält der Administrator den `in.iked`-Daemon an und erhöht anschließend die Privilegstufe auf 2.

```
adm1 # pkill in.iked
adm1 # /usr/lib/inet/in.iked -p 2
Setting privilege level to 2
```

- Der Administrator zeigt die Schlüssel an.

```
adm1 # ikeadm dump preshared
PSKEY: Preshared key (24 bytes): f47cb.../192
LOCIP: AF_INET: port 0, 192.168.116.16 (adm1).
REMIP: AF_INET: port 0, 192.168.13.213 (com1).
```

- Der Administrator meldet sich am Kommunikationssystem an und stellt fest, dass die Schlüssel identisch sind.
- Anschließend setzt der Administrator die Privilegien wieder auf die Basisstufe zurück.

```
# ikeadm set priv base
```

▼ So fügen Sie einen IKE PresharedKey für einen neuen Richtlinieneintrag in `ipsecinit.conf` ein

Wenn Sie IPsec-Richtlinieneinträge hinzufügen, während IPsec und IKE ausgeführt werden, müssen Sie die neue Richtlinie und die neuen IKE-Regeln in den Systemkern einlesen. Wenn Sie mindestens mit Solaris 10 4/09 arbeiten, starten Sie den `policy`-Service neu und aktualisieren den `ike`-Service, nachdem Sie die neuen Schlüssel hinzugefügt haben.

Hinweis – Wenn Sie dieses Verfahren in einer Version vor Solaris 10 4/09 durchführen möchten, schauen Sie sich die Hinweise unter Beispiel 23–3 an.

Bevor Sie beginnen Bei diesem Verfahren wird das folgende Setup vorausgesetzt:

- Das System `enigma` ist wie unter „So konfigurieren Sie IKE mit PresharedKeys“ auf Seite 613 beschrieben eingerichtet.
- Das System `enigma` schützt seinen Datenverkehr mit einem neuen System `ada`.

- Der `in.iked`-Daemon wird auf beiden Systemen ausgeführt.
- Die Schnittstellen der Systeme sind auf beiden Systemen als Einträge in der Datei `/etc/hosts` vorhanden. Ein Beispiel wäre der folgende Eintrag.

```
192.168.15.7 ada
192.168.116.16 enigma
```

  Dieses Verfahren arbeitet auch mit einer IPv6-Adresse in der Datei `/etc/inet/ipnodes`. Ab Solaris 10 6/07 werden IPv6-Einträge in der Datei `/etc/hosts` abgelegt.
- Sie haben auf beiden Systemen einen neuen Richtlinieneintrag in die Datei `/etc/inet/ipsecinit.conf` eingefügt. Die Einträge sind ähnlich den Folgenden:

```
# ipsecinit.conf file for enigma
{laddr enigma raddr ada} ipsec {auth_algs any encr_algs any sa shared}

# ipsecinit.conf file for ada
{laddr ada raddr enigma} ipsec {auth_algs any encr_algs any sa shared}
```

- In der aktuellen Version haben Sie die Syntax der Datei `/etc/inet/ipsecinit.conf` auf beiden Systemen mit folgendem Befehl überprüft:

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

1 Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

---

2 Erstellen Sie auf diesem System Zufallszahlen und einen Schlüssel mit 64 bis 448 Bit.

Ausführliche Informationen finden Sie im Abschnitt „So erzeugen Sie Zufallszahlen auf einem Solaris-System“ auf Seite 543. Informationen zum Erzeugen von Schlüsselmaterial für ein Solaris-System, das mit einem Betriebssystem kommuniziert, das Schlüsselmaterial im ASCII-Format benötigt, finden Sie in Beispiel 23–1.

3 Senden Sie den Schlüssel an den Administrator des remoten Systems.

Beide Administratoren müssen den gleichen PresharedKey zum gleichen Zeitpunkt hinzufügen. Ihr Schlüssel ist nur so sicher wie die Sicherheit Ihres Übertragungsmechanismus. Wir empfehlen einen außerbandigen Mechanismus, z. B. einen Einschreibebrief oder eine geschützte Faxübertragung. Sie können die beiden Systeme auch über eine `ssh`-Sitzung verwalten.

4 Erstellen Sie eine Regel für IKE, um die Schlüssel für `enigma` **und** `ada` **zu verwalten.**

a. Fügen Sie auf dem System `enigma` **der Datei** `/etc/inet/ike/config` **die folgende Regel hinzu:**

```
### ike/config file on enigma, 192.168.116.16

## The rule to communicate with ada

{label "enigma-to-ada"
 local_addr 192.168.116.16
 remote_addr 192.168.15.7
 p1_xform
 {auth_method preshared oakley_group 5 auth_alg sha1 encr_alg blowfish}
 p2_pfs 5
    }
```

b. Fügen Sie auf dem System `ada` **die folgende Regel hinzu:**

```
### ike/config file on ada, 192.168.15.7

## The rule to communicate with enigma

{label "ada-to-enigma"
 local_addr 192.168.15.7
 remote_addr 192.168.116.16
 p1_xform
 {auth_method preshared oakley_group 5 auth_alg sha1 encr_alg blowfish}
 p2_pfs 5
}
```

5 Stellen Sie sicher, dass die IKE PresharedKeys beim erneuten Booten zur Verfügung stehen.

a. Fügen Sie auf dem System `enigma` **der Datei** `/etc/inet/secret/ike.preshared` **die folgenden Informationen hinzu:**

```
# ike.preshared on enigma for the ada interface
#
{ localidtype IP
  localid 192.168.116.16
  remoteidtype IP
  remoteid 192.168.15.7
  # enigma and ada’s shared key in hex (32 - 448 bits required)
  key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d
}
```

b. Fügen Sie auf dem System `ada` **der Datei** `ike.preshared` **die folgenden Informationen hinzu:**

```
# ike.preshared on ada for the enigma interface
#
{ localidtype IP
  localid 192.168.15.7
  remoteidtype IP
  remoteid 192.168.116.16
  # ada and enigma’s shared key in hex (32 - 448 bits required)
  key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d
}
```

6 Starten Sie auf den einzelnen Systemen den Service für die IPsec-Richtlinie neu, damit die neue Schnittstelle ebenfalls geschützt wird.

```
# svcadm restart policy
```

7 Aktualisieren Sie auf den einzelnen Systemen den `ike`-Service.

```
# svcadm refresh ike
```

8 Prüfen Sie, ob die Systeme miteinander kommunizieren können.

Lesen Sie dazu „So prüfen Sie, ob die IKE PresharedKeys identisch sind“ auf Seite 622.

Beispiel 23–3 Hinzufügen eines IKE PresharedKeys für einen neuen IPsec-Richtlinieneintrag

Im folgenden Beispiel fügt der Administrator einen PresharedKey einem System hinzu, auf dem nicht die aktuellste Solaris-Version ausgeführt wird. Der Administrator befolgt das vorstehende Verfahren zur Änderung der Dateien `ike/config` und `ike.preshared`, zur Erstellung von Schlüsseln und zur Herstellung einer Verbindung zum Remote-System. Zum Einlesen der neuen IPsec-Richtlinie und der IKE-Regeln in den Systemkern verwendet der Administrator unterschiedliche Befehle.

- Vor der Erstellung des neuen Schlüssels legt der Administrator die Privilegstufe des `in.iked`-Daemons auf 2 fest.

  ```
  # pkill in.iked
  # /usr/lib/inet/in.iked -p 2
  Setting privilege level to 2
  ```
- Nachdem der Schlüssel an das andere System versendet und dem System hinzugefügt wurde, wählt der Administrator eine niedrigere Privilegstufe aus.

  ```
  # ikeadm set priv base
  ```
- Anschließend liest der Administrator die neue IPsec-Richtlinie in den Systemkern ein.

  ```
  # ipsecconf -a /etc/inet/ipsecinit.conf
  ```
- Zum Schluss werden die neuen IKE-Regeln in den Systemkern eingelesen.

  ```
  # ikeadm read rules
  ```

▼ So prüfen Sie, ob die IKE PresharedKeys identisch sind

Wenn die PresharedKeys auf den kommunizierenden Systemen nicht identisch sind, können die Systeme nicht authentifiziert werden.

Bevor Sie beginnen IPsec wurde konfiguriert und ist zwischen den zu testenden Systemen aktiviert. Sie führen die aktuelle Version (Solaris 10) aus.

Hinweis – Wenn Sie dieses Verfahren in einer Version vor Solaris 10 4/09 durchführen möchten, schauen Sie sich die Hinweise unter Beispiel 23–2 an.

---

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

   Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh` für eine sichere Remoteanmeldung.

   ---

2. **Prüfen Sie auf den einzelnen Systemen die Privilegstufe des `in.iked`-Daemons.**

   ```
   # svcprop -p config/admin_privilege ike
   base
   ```

   - **Falls die Privilegstufe `keymat` lautet, fahren Sie mit Schritt 3 fort.**
   - **Falls die Privilegstufe `base` oder `modkeys` lautet, erhöhen Sie die Stufe.**

     Aktualisieren Sie anschließend das System, und starten Sie den `ike`-Service neu.

     ```
     # svccfg -s ike setprop config/admin_privilege=keymat
     # svcadm refresh ike ; svcadm restart ike
     # svcprop -p config/admin_privilege ike
     keymat
     ```

3. **Zeigen Sie die PresharedKey-Informationen auf beiden Systemen an.**

   ```
   # ikeadm dump preshared
   PSKEY: Preshared key (24 bytes): f47cb.../192
   LOCIP: AF_INET: port 0, 192.168.116.16 (enigma).
   REMIP: AF_INET: port 0, 192.168.13.213 (partym).
   ```

4. **Vergleichen Sie die beiden Speicherauszüge.**

   Sind die PresharedKeys nicht identisch, ersetzen Sie in der Datei `/etc/inet/secret/ike.preshared` einen Schlüssel durch den anderen.

5. **Ändern Sie die Privilegstufe nach Abschluss der Prüfung wieder in den jeweiligen Standardwert der Systeme.**

   ```
   # svccfg -s ike setprop config/admin_privilege=base
   # svcadm restart ike
   ```

Konfiguration von IKE mit PublicKey-Zertifikaten (Übersicht der Schritte)

Die folgende Tabelle enthält Verweise auf Verfahren, in denen beschrieben wird, wie PublicKey-Zertifikaten für IKE erzeugt werden. Außerdem enthalten die Verfahren Informationen zum Beschleunigen und Speichern der Zertifikate auf angehängter Hardware.

Aufgabe	Beschreibung	Siehe
Konfiguration von IKE mit selbst-signierten PublicKey-Zertifikaten	Erstellen und fügen Sie jedem System zwei Zertifikate hinzu: ■ Ein selbst-signiertes Zertifikat ■ Ein PublicKey-Zertifikat vom remoten System	„So konfigurieren Sie IKE mit selbst-signierten PublicKey-Zertifikaten" auf Seite 625
Konfiguration von IKE mit einer PKI-Zertifikatsautorität	Erstellen Sie eine Zertifikatsanforderung und fügen Sie jedem System drei Zertifikate hinzu: ■ Das Zertifikat, das die Zertifikatsautorität (Certificate Authority, CA) aufgrund Ihrer Anforderung erstellt hat ■ Das PublicKey-Zertifikat von der CA ■ Die CRL von der CA	„So konfigurieren Sie IKE mit Zertifikaten, die von einer CA signiert wurden" auf Seite 631
Konfiguration von PublicKey-Zertifikaten auf der lokalen Hardware	Hierzu gehört entweder: ■ Das Erzeugen selbst-signierter Zertifikate auf der lokalen Hardware und anschließend das Hinzufügen des PublicKey von einem remoten System zur Hardware. ■ Das Erzeugen einer Zertifikatsanforderung auf der lokalen Hardware und anschließend das Hinzufügen der PublicKey-Zertifikate von der CA zur Hardware.	„So erzeugen Sie PublicKey-Zertifikate und speichern sie auf angehängter Hardware" auf Seite 636
Aktualisieren der Zertifikat-Widerrücknahmeliste (CRL) von einer PKI	Zugriff auf die CRL an einem zentralen Verteilungspunkt.	„So verarbeiten Sie eine Zertifikat-Rücknahmeliste" auf Seite 640

Konfiguration von IKE mit PublicKey-Zertifikaten

Mit PublicKey-Zertifikaten müssen kommunizierende Systeme kein geheimes außerbandiges Schlüsselmaterial mehr verwenden. Im Gegensatz zu PresharedKeys kann ein PublicKey-Zertifikat auf einem mobilen Computer oder auf einem System verwendet werden, dass neu nummeriert werden kann.

PublicKey-Zertifikate können auch auf angehängter Hardware gespeichert werden. Informationen hierzu finden Sie unter „Konfiguration von IKE zum Suchen angehängter Hardware (Übersicht der Schritte)“ auf Seite 650.

▼ So konfigurieren Sie IKE mit selbst-signierten PublicKey-Zertifikaten

Selbst-designierte Zertifikate erfordern weniger Aufwand als öffentliche Zertifikate von einer CA, lassen sich jedoch nicht einfach skalieren.

1 Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

---

2 Fügen Sie ein selbst-signiertes Zertifikat in die Datenbank `ike.privatekeys` ein.

```
# ikecert certlocal -ks|-kc -m keysize -t keytype \
-D dname -A altname \
[-S validity-start-time] [-F validity-end-time] [-T token-ID]
```

`-ks` — Erstellt ein selbst-signiertes Zertifikat.

`-kc` — Erstellt eine Zertifikatanforderung. Informationen hierzu finden Sie unter „So konfigurieren Sie IKE mit Zertifikaten, die von einer CA signiert wurden“ auf Seite 631.

`-m` *Schlüsselgröße* — Die Größe des Schlüssels. *Schlüsselgröße* kann 512, 1024, 2048, 3072 oder 4096 annehmen.

`-t` *Schlüsseltyp* — Gibt den zu verwendenden Algorithmustyp an. *Schlüsseltyp* kann `rsa-sha1`, `rsa-md5` oder `dsa-sha1` annehmen.

`-D` *dname* — Der X.509-Distinguished Name (DN) für das Zertifikatssubjekt. *dname* hat in der Regel folgende Form: C=Land, O= Organisation, OU= Organisationseinheit, CN= allgemeiner Name. Gültige Tags sind C, O, OU und CN.

`-A` *altname*	Der Alternativname für das Zertifikat. *altname* hat im allgemeinen das Format `Tag=Wert`. Gültige Tags sind `IP`, `DNS`, `email` und `DN`.
`-S` *Gültigkeit-Anfang*	Ist das absolute oder relative Anfangsdatum der Zertifikatsgültigkeit.
`-F` *Gültigkeit-Ende*	Ist das absolute oder relative Enddatum der Zertifikatsgültigkeit.
`-T` *Token-ID*	Ermöglicht, dass ein PKCS&;#11-Hardwaretoken die Schlüssel erzeugt. Die Zertifikate werden dann auf der Hardware gespeichert.

a. **Der Befehl auf dem System `partym` sieht in etwa wie folgt aus:**

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
-A IP=192.168.13.213
Creating software private keys.
  Writing private key to file /etc/inet/secret/ike.privatekeys/0.
Enabling external key providers - done.
Acquiring private keys for signing - done.
Certificate:
 Proceeding with the signing operation.
 Certificate generated successfully (.../publickeys/0)
Finished successfully.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIICLTCCAZagAwIBAgIBATANBgkqhkiG9w0BAQQFADBNMQswCQYDVQQGEwJVUzEX
...
6sKTxpg4GP3GkQGcd0r1rhW/3yaWBkDwOdFCqEUyffzU
-----END X509 CERTIFICATE-----
```

b. **Der Befehl auf dem System `enigma` sieht in etwa wie folgt aus:**

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax" \
-A IP=192.168.116.16
Creating software private keys.
  ...
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIICKDCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQQFADBJMQswCQYDVQQGEwJVUzEV
...
jpxfLM98xyFVyLCbkr3dZ3Tvxvi732BXePKF2A==
-----END X509 CERTIFICATE-----
```

3 **Speichern Sie das Zertifikat und senden Sie es an das remote System.**

Sie können das Zertifikat in eine E-Mail einfügen.

a. **So können Sie das folgende `partym`-Zertifikat an den Administrator von `enigma` senden:**

```
To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIICLTCCAZagAwIBAgIBATANBgkqhkiG9w0BAQQFADBNMQswCQYDVQQGEwJVUzEX
...
6sKTxpg4GP3GkQGcd0r1rhW/3yaWBkDwOdFCqEUyffzU
-----END X509 CERTIFICATE-----
```

b. **Der Administrator von `enigma` sendet Ihnen das folgende `enigma`-Zertifikat:**

```
To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIICKDCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQQFADBJMQswCQYDVQQGEwJVUzEV
...
jpxfLM98xyFVyLCbkr3dZ3Tvxvi732BXePKF2A==
-----END X509 CERTIFICATE-----
```

4 **</remark>Fügen Sie auf jedem System das empfangene Zertifikat ein.**

a. **Kopieren Sie den PublicKey aus der E-Mail des Administrators.**

b. **Geben Sie den Befehl `ikecert certdb -a` ein, und drücken Sie die Eingabetaste.**

Wenn Sie die Eingabetaste drücken, werden keine Eingabeaufforderungen angezeigt.

```
# ikecert certdb -a        Press the Return key
```

c. **Fügen Sie den PublicKey ein, und drücken Sie die Eingabetaste. Drücken Sie dann Strg-D, um den Eintrag zu beenden.**

```
-----BEGIN X509 CERTIFICATE-----
MIIC...
...
----END X509 CERTIFICATE-----      Press the Return key
<Control>-D
```

5 **Prüfen Sie gemeinsam mit dem anderen Administrator, dass das Zertifikat von diesem Administrator stammt.**

Beispielsweise können Sie mit dem anderen Administrator telefonieren und die Werte des PublicKey-Hash vergleichen. Das PublicKey-Hash für das gemeinsam genutzte Zertifikat muss auf beiden Systemen gleich sein.

a. **Listen Sie das gespeicherte Zertifikat auf Ihrem System auf.**

So befindet sich das öffentliche Zertifikat z. B. auf dem System `partym` in Slot 1 und das private Zertifikat in Slot 0.

```
partym # ikecert certdb -l
Certificate Slot Name: 0   Type: rsa-md5      Private Key
    Subject Name: <C=US, O=PartyCompany, OU=US-Partym, CN=Partym>
    Key Size: 1024
    Public key hash: B2BD13FCE95FD27ECE6D2DCD0DE760E2

Certificate Slot Name: 1   Type: rsa-md5       Public Certificate
    (Private key in certlocal slot 0)      Points to certificate's private key
    Subject Name: <C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax>
    Key Size: 1024
    Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

b. Vergleichen Sie diesen Wert mit dem PublicKey-Hash auf dem System `enigma`.

Sie können den PublicKey-Hash über das Telefon vorlesen.

```
enigma # ikecert certdb -l
Certificate Slot Name: 4   Type: rsa-md5      Private Key
    Subject Name: <C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax>
    Key Size: 1024
    Public key hash: DF3F108F6AC669C88C6BD026B0FCE3A0

Certificate Slot Name: 5   Type: rsa-md5      Public Certificate
    (Private key in certlocal slot 4)
    Subject Name: <C=US, O=PartyCompany, OU=US-Partym, CN=Partym>
    Key Size: 1024
    Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

6 Richten Sie auf den Systemen eine Vertrauensstellung für die beide Zertifikate ein.

Ändern Sie die Datei `/etc/inet/ike/config` so, dass die Zertifikate erkannt werden.

Der Administrator des remoten Systems stellt die Werte für die Parameter `cert_trust`, `remote_addr` und `remote_id` zur Verfügung.

a. Auf dem System `partym` enthält die `ike/config`-Datei Folgendes:

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

# Verified remote address and remote ID
# Verified public key hash per telephone call from administrator
cert_trust "192.168.13.213"      Local system's certificate Subject Alt Name
cert_trust "192.168.116.16"      Remote system's certificate Subject Alt Name

## Parameters that may also show up in rules.

p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 5

{
 label "US-partym to JA-enigmax"
 local_id_type dn
 local_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
 remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

 local_addr  192.168.13.213
 remote_addr 192.168.116.16

 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

b. **Geben Sie auf dem System `enigma` die `enigma`-Werte für lokale Parameter in die Datei `ike/config` ein.**

   Für die remoten Parameter verwenden Sie `partym`-Werte. Achten Sie darauf, dass der Wert für das Schlüsselwort `label` einmalig ist. Der Wert muss sich von dem `label`-Wert des remoten Systems unterscheiden.

   ```
   ...
   {
    label "JA-enigmax to US-partym"
    local_id_type dn
    local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
    remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

    local_addr  192.168.116.16
    remote_addr 192.168.13.213
   ...
   ```

Beispiel 23–4 Prüfen Sie, ob das Zertifikat vom anderen Administrator gültig ist

In diesem Beispiel verwenden die Administratoren den „Subject Name“ um sicherzustellen, dass die Zertifikate identisch sind.

Der erste Administrator speichert die Ausgabe des Erzeugens und Auflistens des Zertifikats in einer Datei. Da die Ausgabe des `ikecert`-Befehls in den Standardfehler druckt, leitet der Administrator den Standardfehler an die Datei um.

```
sys1# cd /
sys1# ikecert certlocal -ks -m1024 -t rsa-md5 \
-D"C=US, O=TestCo, CN=Co2Sys" 2>/tmp/for_co2sys
Certificate added to database.
sys1# ikecert certdb -l "C=US, O=TestCo, CN=Co2Sys" 2>>/tmp/for_co2sys
```

Der Administrator überprüft den Inhalt der Datei.

```
sys1# cat /tmp/for_co2sys
Creating private key.
-----BEGIN X509 CERTIFICATE-----
MIIB7TCCAVagAwIBAgIEZkHfOTANBgkqhkiG9w0BAQQFADAxMQwwCgYDVQQGEwNV
U0ExEDAOBgNVBAoMB3Rlc3RfY28xDzANBgNVBAMTBkVuaWdtYTAeFw0wODAxMTUx
OTI1MjBaFw0xMjAxMTUxOTI1MjBaMDExDDAKBgNVBAYTA1VTQTEQMA4GA1UECgwH
dGVzdF9jbzEPMA0GA1UEAxMGRW5pZ21hMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQCPxGv0rUzHMnFtkx9uwYuPiWbftmWfa9iDt6ELOEuw3zlboy2qtuRUZohz
FIbCxAJevdCY6a+pktvYy3/2nJL0WATObO5T0FKn3F0bphajinLYbyCrYhEzD9E2
gkiT2D9/ttbSiMvi9usphprEDcLAFaWgCJiHnKPBEkjC0vhA3wIDAQABoxIwEDAO
BgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEEBQADgYEAL/q6xgweylGQylqLCwzN
5PIpjfzsNPf3saTyh3VplwEOW6WTHwRQT17IO/1Oc6Jnz9Mr0ZrbHWDXq+1sx180
F8+DMW1Qv1UR/lGMq3ufDG3qedmSN6txDF8qLlPCUML0YL8m4oGdewqGb+78aPyE
Y/cJRsK1hWbYyseqcIkjj5k=
-----END X509 CERTIFICATE-----
Certificate Slot Name: 2   Key Type: rsa
        (Private key in certlocal slot 2)
        Subject Name: <C=US, O=TestCo, CN=Co2Sys>
        Key Size: 1024
```

```
        Public key hash: C46DE77EF09084CE2B7D9C70479D77FF
```

Dann sendet der Administrator die Datei in einer E-Mail an den zweiten Administrator.

Der zweite Administrator fügt die Datei in ein sicheres Verzeichnis ein und importiert dann das Zertifikat aus der Datei.

```
sys2# cd /
sys2# ikecert certdb -a < /sec/co2sys
```

Der Befehl `ikecert` importiert nur den Text zwischen den Zeilen `-----BEGIN` und `-----END`. Der Administrator überprüft, ob das lokale Zertifikat den gleichen öffentlichen Key-Hash wie in der Datei `co2sys` aufweist.

```
sys2# ikecert certdb -l
Certificate Slot Name: 1   Key Type: rsa
        (Private key in certlocal slot 1)
        Subject Name: <C=US, O=TestCo, CN=Co2Sys>
        Key Size: 1024
        Public key hash: C46DE77EF09084CE2B7D9C70479D77FF
```

Um sicherzustellen, dass der erste Administrator diese E-Mail gesendet hat, telefoniert der zweite Administrator, um die Richtigkeit des „Subject Name" des Zertifikats zu bestätigen.

Beispiel 23–5 Einrichten von Anfangs- und Enddatum für die Gültigkeit eines Zertifikats

In diesem Beispiel gibt der Administrator des Systems `partym` vor, wie lange ein Zertifikat gültig ist. Das Zertifikat ist um 2 1/2 Tage zurückdatiert und gilt für vier Jahre und sechs Monate ab dem Erstellungsdatum.

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
-A IP=192.168.13.213 \
-S -2d12h -F +4y6m
```

Der Administrator des Systems `enigma` gibt die Daten an, innerhalb denen das Zertifikat gültig ist. Das Zertifikat wurde um zwei Tage zurückdatiert und gilt bis Mitternacht am 31. Dezember 2010.

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax" \
-A IP=192.168.116.16 \
-S -2d -F "12/31/2010 12:00 AM"
```

▼ So konfigurieren Sie IKE mit Zertifikaten, die von einer CA signiert wurden

Öffentliche Zertifikate einer Zertifikatsautorität (CA) machen eine Aushandlung mit einer außenstehenden Organisation erforderlich. Diese Zertifikate können leicht skaliert werden, so dass zahlreiche miteinander kommunizierende Systeme geschützt werden können.

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

   Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

   ---

2. **Geben Sie den Befehl `ikecert certlocal -kc` ein, um ein Zertifikat anzufordern.**

   Eine Beschreibung der Argumente dieses Befehls finden Sie in Schritt 2 unter „So konfigurieren Sie IKE mit selbst-signierten PublicKey-Zertifikaten" auf Seite 625.

   ```
   # ikecert certlocal -kc -m keysize -t keytype \
   -D dname -A altname
   ```

   a. **Der folgende Befehl erstellt eine Zertifikat-Anforderung auf dem System `partym`:**

   ```
   # ikecert certlocal -kc -m 1024 -t rsa-md5 \
   > -D "C=US, O=PartyCompany\, Inc., OU=US-Partym, CN=Partym" \
   > -A "DN=C=US, O=PartyCompany\, Inc., OU=US-Partym"
   Creating software private keys.
     Writing private key to file /etc/inet/secret/ike.privatekeys/2.
   Enabling external key providers - done.
   Certificate Request:
     Proceeding with the signing operation.
     Certificate request generated successfully (.../publickeys/0)
   Finished successfully.
   -----BEGIN CERTIFICATE REQUEST-----
   MIIByjCCATMCAQAwUzELMAkGA1UEBhMCVVMxHTAbBgNVBAoTFEV4YW1wbGVDb21w
   ...
   lcM+tw0ThRrfuJX9t/Qa1R/KxRlMA3zckO80mO9X
   -----END CERTIFICATE REQUEST-----
   ```

   b. **Der folgende Befehl erstellt eine Zertifikat-Anforderung auf dem System `enigma`:**

   ```
   # ikecert certlocal -kc -m 1024 -t rsa-md5 \
   > -D "C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax, CN=Enigmax" \
   > -A "DN=C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax"
   ```

```
Creating software private keys.
...
Finished successfully.
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
...
8qlqdjaStLGfhDOO
-----END CERTIFICATE REQUEST-----
```

3 Übermitteln Sie die Zertifikat-Anforderung an eine PKI-Organisation.

Die PKI-Organisation teilt Ihnen mit, wie die Zertifikat-Anforderung übermittelt werden soll. Die meisten Organisationen verfügen über eine Website mit einem Übertragungsformular. Das Formular fordert einen Beweis, dass die Übertragung legitim ist. In der Regel fügen Sie Ihre Zertifikat-Anforderung in das Formular ein. Nachdem Ihre Anforderung von der Organisation überprüft wurde, stellt sie die folgenden zwei Zertifikatsobjekte sowie eine Liste zurückgenommenen Zertifikate aus:

- Ihr PublicKey-Zertifikat – Dieses Zertifikat basiert auf der Anforderung, die Sie an die Organisation übermittelt haben. Die von Ihnen übermittelte Anforderung ist Teil dieses PublicKey-Zertifikats. Das Zertifikat identifiziert Sie eindeutig.
- Eine Zertifikatsautorität – Die Signatur der Organisation. Die CA prüft, ob Ihr PublicKey-Zertifikat echt und unverfälscht ist.
- Eine Zertifikat-Rücknahmeliste (Certificate Revocation List, CRL) – Die aktuelle Liste der Zertifikate, die von der Organisation zurückgenommen wurden. Die CRL wird nicht separat als ein Zertifikatsobjekt gesendet, wenn der Zugriff auf die CRL in das PublicKey-Zertifikat eingebettet ist.

  Ist ein URI für die CRL in das PublicKey-Zertifikat eingebettet, kann IKE die CRL automatisch für Sie abrufen. Entsprechend gilt, ist ein DN-Eintrag (Verzeichnisname auf einem LDAP-Server) in das PublicKey-Zertifikat eingebettet, kann IKE die CRL vom angegebenen LDAP-Server abrufen und zwischenspeichern.

  Ein Beispiel eines eingebetteten URI und eines eingebetteten DN-Eintrags in einem PublicKey-Zertifikat finden Sie unter „So verarbeiten Sie eine Zertifikat-Rücknahmeliste“ auf Seite 640.

4 Fügen Sie Ihrem System alle Zertifikate hinzu.

Mit der Option `-a` des Befehls `ikecert certdb -a` fügen Sie das eingefügte Objekt der entsprechenden Zertifikatdatenbank Ihres Systems hinzu. Weitere Informationen finden Sie unter „IKE mit PublicKey-Zertifikaten“ auf Seite 607.

a. Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

b. **Fügen Sie das PublicKey-Zertifikat hinzu, das Sie von der PKI -Organisation empfangen haben.**

```
# ikecert certdb -a
       Press the Return key
       Paste the certificate:
-----BEGIN X509 CERTIFICATE-----
...
-----END X509 CERTIFICATE----
       Press the Return key
<Control>-D
```

c. **Fügen Sie die CA von der PKI-Organisation hinzu.**

```
# ikecert certdb -a
       Press the Return key
       Paste the CA:
-----BEGIN X509 CERTIFICATE-----
...
-----END X509 CERTIFICATE----
       Press the Return key
<Control>-D
```

d. **Wenn die PKI-Organisation eine Liste der zurückgenommenen Zertifikate gesendet hat, fügen Sie die CRL zur `certrldb`-Datenbank hinzu:**

```
# ikecert certrldb -a
       Press the Return key
       Paste the CRL:
-----BEGIN CRL-----
...
-----END CRL----
       Press the Return key
<Control>-D
```

5 **Geben Sie das Schlüsselwort `cert_root` ein, um die PKI-Organisation in der Datei `/etc/inet/ike/config` zu identifizieren.**

Verwenden Sie den von der PKI-Organisation angegebenen Namen.

a. **Die Datei `ike/config` auf dem System `partym` könnte wie folgt aussehen:**

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

## Parameters that may also show up in rules.

p1_xform
 { auth_method rsa_sig oakley_group 1 auth_alg sha1 encr_alg des }
```

```
p2_pfs 2

{
 label "US-partym to JA-enigmax - Example PKI"
 local_id_type dn
 local_id  "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
 remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

 local_addr  192.168.13.213
 remote_addr 192.168.116.16

 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

Hinweis – Alle Argumente für den Parameter `auth_method` müssen sich auf der gleichen Zeile befinden.

---

b. **Erstellen Sie eine ähnliche Datei auf dem System `enigma`.**

Beachten Sie bei der Datei `enigma` `ike/config` Folgendes:

- Fügen Sie den gleichen `cert_root`-Wert hinzu.
- Verwenden Sie `enigma`-Werte für lokale Parameter.
- Verwenden Sie `partym`-Werte für remote Parameter.
- Erstellen Sie einen einmaligen Wert für das Schlüsselwort `label.` Der Wert muss sich von dem `label`-Wert des remoten Systems unterscheiden.

```
...
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"
...
{
 label "JA-enigmax to US-partym - Example PKI"
 local_id_type dn
 local_id   "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
 remote_id  "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

 local_addr  192.168.116.16
 remote_addr 192.168.13.213
...
```

6 **Weisen Sie IKE an, wie die CRLs verarbeitet werden sollen.**

Wählen Sie die geeignete Option:

- **Keine CRL verfügbar**

  Wenn die PKI-Organisation keine CRL zur Verfügung stellt, fügen Sie das Schlüsselwort `ignore_crls` zur `ike/config` -Datei hinzu.

  ```
  # Trusted root cert
  ...
  ```

```
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example,...
ignore_crls
...
```

Das Schlüsselwort `ignore_crls` weist IKE an, nicht nach CRLs zu suchen.

- **CRL verfügbar**

  Wenn die PKI-Organisation einen zentralen Verteilungspunkt für CRLs bereitstellt, können Sie in der Datei `ike/config` auf diesen Speicherort verweisen.

  Beispiele finden Sie unter „So verarbeiten Sie eine Zertifikat-Rücknahmeliste“ auf Seite 640.

Beispiel 23–6 Verwenden von `rsa_encrypt` bei der Konfiguration von IKE

Wenn Sie `auth_method rsa_encrypt` in der `ike/config`-Datei angeben, müssen Sie das Zertifikat des Peers zur `publickeys`-Datenbank hinzufügen.

1. Senden Sie das Zertifikat an den Administrator des remoten Systems.

   Sie können das Zertifikat in eine E-Mail einfügen.

   Der Administrator von `partym` sendet Ihnen die folgende E-Mail:

   ```
   To: admin@ja.enigmaexample.com
   From: admin@us.partyexample.com
   Message: -----BEGIN X509 CERTIFICATE-----
   MII...
   ----END X509 CERTIFICATE-----
   ```

   Der Administrator von `enigma` sendet die folgende E-Mail:

   ```
   To: admin@us.partyexample.com
   From: admin@ja.enigmaexample.com
   Message: -----BEGIN X509 CERTIFICATE-----
   MII
   ...
   -----END X509 CERTIFICATE-----
   ```

2. Fügen Sie das per E-Mail gesendete Zertifikat auf beiden Systemen zur lokalen `publickeys`-Datenbank hinzu.

   ```
   # ikecert certdb -a
       Press the Return key
   -----BEGIN X509 CERTIFICATE-----
   MII...
   -----END X509 CERTIFICATE-----
       Press the Return key
   <Control>-D
   ```

Die Authentifizierungsmethode für die RSA-Verschlüsselung verbirgt Identitäten in IKE vor möglichen Lauschangriffen. Da die `rsa_encrypt`-Methode die Identität des Peers verbirgt, kann IKE das Zertifikat des Peers nicht abrufen. Aus diesem Grund erfordert die `rsa_encrypt`-Methode, dass die IKE-Peers die PublicKeys des jeweils anderen Systems kennen.

Wenn Sie den `auth_method` `rsa_encrypt` in der `/etc/inet/ike/config`-Datei angeben, müssen Sie das Zertifikat des Peers zur `publickeys`-Datenbank hinzufügen. Die `publickeys`-Datenbank enthält dann drei Zertifikate für jedes kommunizierenden Systempaar:

- Ihr PublicKey-Zertifikat
- Das CA-Zertifikat
- Das PublicKey-Zertifikat des Peer

Fehlerbehebung – Die IKE-Nutzlast, zu der auch die drei Zertifikate gehören, könnte zu groß werden, so dass eine Verschlüsselung durch `rsa_encrypt` nicht mehr möglich ist. Fehlermeldungen wie „Autorisierung fehlgeschlagen" und „Fehlerhafte Nutzlast" deuten darauf hin, dass die `rsa_encrypt`-Methode nicht die gesamte Nutzlast verschlüsseln konnte. Reduzieren Sie die Nutzlastgröße mit einer Methode wie z. B. `rsa_sig`, die nur zwei Zertifikate erfordert.

▼ So erzeugen Sie PublicKey-Zertifikate und speichern sie auf angehängter Hardware

Das Erzeugen von PublicKey-Zertifikaten und das Speichern dieser Zertifikate auf angehängter Hardware ähnelt dem Erzeugen von PublicKey-Zertifikaten und dem Speichern dieser Zertifikate auf Ihrem System. Auf der Hardware müssen die Befehle `ikecert certlocal` und `ikecert certdb` die Hardware identifizieren. Die Option `-T` mit der Token-ID identifiziert die Hardware gegenüber den Befehlen.

Bevor Sie beginnen

- Die Hardware muss konfiguriert sein.
- Die Hardware verwendet die `/usr/lib/libpkcs11.so`-Bibliothek, es sei denn, das Schlüsselwort `pkcs11_path` in der `/etc/inet/ike/config`-Datei verweist auf eine andere Bibliothek. Die Bibliothek muss gemäß dem folgenden Standard implementiert sein: RSA Security Inc. PKCS&;#11 Cryptographic Token Interface (Cryptoki), das heißt, eine PKCS&;#11-Bibliothek.

  Informationen zum Setup finden Sie unter „So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 4000-Board" auf Seite 652.

1 Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

---

2 Erzeugen Sie ein selbst-signiertes Zertifikat oder eine Zertifikat-Anforderung, und geben Sie die Token-ID an.

Wählen Sie eine der folgenden Optionen:

Hinweis – Für RSA unterstützt das Sun Crypto Accelerator 4000-Board Schlüssel bis zu 2048 Bit. Für DSA unterstützt dieses Board Schlüssel bis zu 1024 Bit.

- **Bei einem selbst-signiertem Zertifikate verwenden Sie die folgende Syntax.**

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
> -a -T dca0-accel-stor IP=192.168.116.16
Creating hardware private keys.
Enter PIN for PKCS#11 token:      Type user:password
```

  Das Argument für die Option `-T` ist die Token-ID des angehängten Sun Crypto Accelerator 4000-Boards.

- **Bei einer Zertifikat-Anforderung verwenden Sie die folgende Syntax.**

```
# ikecert certlocal -kc -m 1024 -t rsa-md5 \
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
> -a -T dca0-accel-stor IP=192.168.116.16
Creating hardware private keys.
Enter PIN for PKCS#11 token:      Type user:password
```

Eine Beschreibung der Argumente für den Befehl `ikecert` finden Sie in der Manpage `ikecert`(1M).

3 Geben Sie an der Eingabeaufforderung für eine PIN den Sun Crypto Accelerator 4000-Benutzer, einen Doppelpunkt und das Passwort des Benutzers ein.

Hat das Sun Crypto Accelerator 4000-Board beispielsweise den Benutzer `ikemgr`, dessen Passwort `rgm4tigt` lautet, geben Sie Folgendes ein:

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt
```

Hinweis – Die PIN-Antwort wird auf dem Datenträger *als Reintext* gespeichert.

Nachdem Sie das Passwort eingegeben haben, druckt das Zertifikat Folgendes:

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt
-----BEGIN X509 CERTIFICATE-----
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
...
oKUDBbZ9O/pLWYGr
-----END X509 CERTIFICATE-----
```

4. **Senden Sie Ihr Zertifikat an die andere Partei.**

   Wählen Sie eine der folgenden Optionen:

   - **Senden Sie das selbst-signierte Zertifikat an das remote System.**

     Sie können das Zertifikat in eine E-Mail einfügen.

   - **Senden Sie die Zertifikat-Anforderung an eine Organisation, die PKI verarbeitet.**

     Folgen Sie den Anweisungen der PKI-Organisation zur Übermittlung der Zertifikat-Anforderung. Ausführliche Anweisungen finden Sie in Schritt 3 unter „So konfigurieren Sie IKE mit Zertifikaten, die von einer CA signiert wurden“ auf Seite 631.

5. **Ändern Sie auf Ihrem System die Datei `/etc/inet/ike/config`, so dass die Zertifikate erkannt werden.**

   Wählen Sie eine der folgenden Optionen.

   - **Selbst-signiertes Zertifikat**

     Verwenden Sie die vom Administrator des remoten Systems bereitgestellten Werte für die Parameter `cert_trust`, `remote_id` und `remote_addr`. Auf dem System `enigma` enthält die `ike/config`-Datei Folgendes:

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

cert_trust "192.168.116.16"        Local system's certificate Subject Alt Name
cert_trust "192.168.13.213"        Remote system's certificate Subject Alt name


# Solaris 10 1/06 release: default path does not have to be typed in
#pkcs11_path "/usr/lib/libpkcs11.so"       Hardware connection

# Solaris 10 release: use this path
#pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
...
{
 label "JA-enigmax to US-partym"
 local_id_type dn
 local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
```

```
 remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

 local_addr  192.168.116.16
 remote_addr 192.168.13.213

 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

- **Zertifikat-Anforderung**

  Geben Sie den von der PKI-Organisation bereitgestellten Namen als Wert für das Schlüsselwort `cert_root` ein. Die Datei `ike/config` könnte auf dem System `enigma` wie folgt aussehen:

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

# Solaris 10 1/06 release: default path does not have to be typed in
#pkcs11_path "/usr/lib/libpkcs11.so"      Hardware connection

# Solaris 10 release: use this path
#pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
...
{
 label "JA-enigmax to US-partym - Example PKI"
 local_id_type dn
 local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
 remote_id  "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

 local_addr  192.168.116.16
 remote_addr 192.168.13.213

 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

6 Speichern Sie die Zertifikate der anderen Partei auf der angehängten Hardware.

Antworten Sie auf die PIN-Anforderung, wie Sie in Schritt 3 geantwortet haben.

Hinweis – Sie *müssen* die PublicKey-Zertifikate auf der angehängten Hardware speichern, die Ihren PrivateKey erstellt hat.

- **Selbst-signiertes Zertifikat.**

  Fügen Sie das selbst-signierte Zertifikat des remoten Systems hinzu. In diesem Beispiel wird das Zertifikat in der Datei DCA.ACCEL.STOR.CERT gespeichert.

  ```
  # ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CERT
  Enter PIN for PKCS#11 token:       Type user:password
  ```

  Wenn das selbst-signierte Zertifikat `rsa_encrypt` als Wert für den Parameter `auth_method` verwendet, fügen Sie das Zertifikat des Peers zum Hardwarespeicher hinzu.

- **Zertifikate von einer PKI-Organisation.**

  Fügen Sie die von der Organisation als Antwort auf Ihre Zertifikate-Anforderung erzeugten Zertifikate und die Zertifikatsautorität (CA) hinzu.

  ```
  # ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CERT
  Enter PIN for PKCS#11 token:       Type user:password

  # ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CA.CERT
  Enter PIN for PKCS#11 token:       Type user:password
  ```

  Informationen zum Hinzufügen der Zertifikat-Rücknahmeliste (CRL) von der PKI-Organisation finden Sie unter „So verarbeiten Sie eine Zertifikat-Rücknahmeliste“ auf Seite 640.

▼ So verarbeiten Sie eine Zertifikat-Rücknahmeliste

Eine Zertifikat-Rücknahmeliste (Certificate Revocation List, CRL) enthält veraltete und sicherheitsgefährdete Zertifikate einer Zertifikatsautorität. Es gibt vier Möglichkeiten, CRLs zu verarbeiten.

- Sie müssen IKE anweisen, CRLs zu ignorieren, wenn Ihre CA-Organisation keine CRLs ausgibt. Diese Option wird in Schritt 6 unter „So konfigurieren Sie IKE mit Zertifikaten, die von einer CA signiert wurden“ auf Seite 631 gezeigt.
- Sie können IKE anweisen, über einen URI (Uniform Resource Indicator), dessen Adresse in das PublicKey-Zertifikat von der CA eingebettet ist, auf die CRLs zugreifen.
- Sie können IKE anweisen, über einen LDAP-Server, dessen DN-Eintrag (Verzeichnisname) in das PublicKey-Zertifikat von der CA eingebettet ist, auf die CRLs zugreifen.
- Sie können die CRL als ein Argument für den Befehl `ikecert certrldb` angeben. Siehe Beispiel 23–7.

Im folgenden Verfahren wird beschrieben, wie Sie IKE anweisen, CRLs von einem zentralen Verteilungspunkt aus zu verwenden.

1 Zeigen Sie die von der CA empfangenen Zertifikate an.

```
# ikecert certdb -lv certspec
```

`-l` Listet die Zertifikate in der IKE-Zertifikatsdatenbank auf.

`-v` Listet die Zertifikate im ausführlichen Modus auf. Verwenden Sie diese Option nur nach sorgfältigen Überlegungen.

certspec Ein Muster, das Entsprechungen für ein Zertifikat in der IKE-Zertifikatsdatenbank findet.

Das folgende Zertifikat wurde beispielsweise von Sun Microsystems herausgegeben. Bestimmte Einzelheiten wurden geändert.

```
# ikecert certdb -lv example-protect.sun.com
Certificate Slot Name: 0   Type: dsa-sha1
   (Private key in certlocal slot 0)
 Subject Name: <O=Sun Microsystems Inc, CN=example-protect.sun.com>
 Issuer Name: <CN=Sun Microsystems Inc CA (Cl B), O=Sun Microsystems Inc>
 SerialNumber: 14000D93
   Validity:
      Not Valid Before: 2002 Jul 19th, 21:11:11 GMT
      Not Valid After:  2005 Jul 18th, 21:11:11 GMT
   Public Key Info:
      Public Modulus  (n) (2048 bits): C575A...A5
      Public Exponent (e) (  24 bits): 010001
   Extensions:
      Subject Alternative Names:
              DNS = example-protect.sun.com
      Key Usage: DigitalSignature KeyEncipherment
      [CRITICAL]
   CRL Distribution Points:
      Full Name:
         URI = #Ihttp://www.sun.com/pki/pkismica.crl#i
         DN = <CN=Sun Microsystems Inc CA (Cl B), O=Sun Microsystems Inc>
      CRL Issuer:
      Authority Key ID:
      Key ID:              4F ... 6B
      SubjectKeyID:        A5 ... FD
      Certificate Policies
      Authority Information Access
```

Beachten Sie den Eintrag `CRL Distribution Points.` Der URI-Eintrag kennzeichnet, dass die CRL dieser Organisation im Web verfügbar ist. Der DN-Eintrag gibt an, dass die CRL auf einem LDAP-Server zur Verfügung steht. Nachdem IKE einmal auf die CRL zugegriffen hat, wird sie zur weiteren Verwendung zwischengespeichert.

Um auf die CRL zuzugreifen, müssen Sie einen Verteilungspunkt erreichen.

2 Wählen Sie eine der folgenden Methoden, um auf die CRL an einem zentralen Verteilungspunkt zuzugreifen.

- **Mithilfe des URI.**

  Fügen Sie das Schlüsselwort `use_http` zur Datei `/etc/inet/ike/config` des Hosts hinzu. Die Datei `ike/config` ähnelt dann Folgendem:

  ```
  # Use CRL from organization's URI
  use_http
  ...
  ```

- **Mithilfe eines Web-Proxy.**

  Fügen Sie das Schlüsselwort `proxy` zur `ike/config`-Datei hinzu. Das Schlüsselwort `proxy` akzeptiert eine URL als Argument, wie in dem folgenden Beispiel:

  ```
  # Use own web proxy
  proxy "http://proxy1:8080"
  ```

- **Mithilfe eines LDAP-Servers.**

  Geben Sie den LDAP-Server als Argument für das Schlüsselwort `ldap-list` in die `/etc/inet/ike/config`-Datei des Hosts ein. Ihre Organisation stellt den Namen des LDAP-Servers zur Verfügung. Der Eintrag in der `ike/config`-Datei würde Folgendem ähneln:

  ```
  # Use CRL from organization's LDAP
  ldap-list "ldap1.sun.com:389,ldap2.sun.com"
  ...
  ```

IKE ruft die CRL ab und speichert die CRL zwischen, bis das Zertifikat abgelaufen ist.

Beispiel 23–7 Einfügen einer CRL in die lokale `certrldb`-Datenbank

Wenn die CRL einer PKI-Organisation nicht an einem zentralen Verteilungspunkt zur Verfügung steht, können Sie die CRL der zur lokalen `certrldb`-Datenbank manuell hinzufügen. Folgen Sie den Anweisungen der PKI-Organisation zum Extrahieren der CRL in eine Datei, dann fügen Sie die CRL mit dem Befehl `ikecert certrldb -a` zur Datenbank hinzu.

```
# ikecert certrldb -a < Sun.Cert.CRL
```

Konfiguration von IKE für mobile Systeme (Übersicht der Schritte)

Die folgende Tabelle enthält Verweise auf Verfahren, in denen beschrieben wird, wie IKE so konfiguriert wird, dass Systeme verarbeitet werden können, die sich remote bei einem zentralen Standort anmelden.

Aufgabe	Beschreibung	Siehe
Kommunizieren mit einem zentralen Standort von einem Offsite-Standort	Ermöglichen Sie es Offsite-Systemen, mit einem zentralen Standort zu kommunizieren. Bei Offsite-Systemen kann es sich um mobile Systeme handeln.	„So konfigurieren Sie IKE für Offsite-Systeme" auf Seite 643
Verwenden eines Root-Zertifikat und IKE auf einem zentralen System, das Datenverkehr von mobilen Systemen akzeptiert	Konfigurieren Sie ein Gateway-Systems, so dass es IPsec-Verkehr von einem System akzeptiert, das nicht über eine feststehende IP-Adresse verfügt.	Beispiel 23–8
Verwenden eines Root-Zertifikat und IKE auf einem System, das nicht über eine feststehende IP-Adresse verfügt	Konfigurieren Sie ein mobiles System, um seinen Datenverkehr mit einem zentralen Standort, z. B. das Unternehmenshauptbüro zu schützen.	Beispiel 23–9
Verwenden von selbst-signierten Zertifikaten und IKE auf einem zentralen System, das Datenverkehr von mobilen Systemen akzeptiert	Konfigurieren Sie ein Gateway-System mit selbst-signierten Zertifikaten, so dass es von IPsec-Verkehr von einem mobilen System akzeptiert.	Beispiel 23–10
Verwenden von selbst-signierten Zertifikaten und IKE auf einem System, das nicht über eine feststehende IP-Adresse verfügt	Konfigurieren Sie ein mobilen System mit selbst-signierten Zertifikaten, so dass sein Verkehr mit einem zentralen Standort geschützt wird.	Beispiel 23–11

Konfiguration von IKE für mobile Systeme

Wenn Heimbüros und mobile Laptops ordnungsgemäß konfiguriert wurden, können IPsec und IKE die Kommunikation mit den Computern am Unternehmenssitz schützen. Eine umfassende IPsec-Richtlinie, kombiniert mit einer PublicKey-Authentifizierungsmethode, bietet Offsite-Systemen die Möglichkeit, ihren Datenverkehr mit einem zentralen System zu schützen.

▼ So konfigurieren Sie IKE für Offsite-Systeme

IPsec und IKE erfordern eine einmalige ID, um Quelle und Ziel eindeutig identifizieren zu können. Bei offsite oder mobilen Systemen, die nicht über eine einmalige IP-Adresse verfügen, müssen Sie einen anderen ID-Typ verwenden. Beispielsweise kann ein System eindeutig mit ID-Typen wie `DNS`, `DN` oder `E-Mail` identifiziert werden.

Offsite oder mobile Systeme, die über einmalige IP-Adressen verfügen, werden dennoch besser mit einem anderen ID-Typ konfiguriert. Wenn die Systeme z. B. versuchen, über eine NAT-Box eine Verbindung mit einem zentralen Standort herzustellen, werden deren einmalige Adressen nicht verwendet. Eine NAT-Box weist eine zufällige IP-Adresse zu, die das zentrale System nicht erkennen würde.

PresharedKeys können ebenfalls nicht als Authentifizierungsmechanismus für mobile Systeme eingesetzt werden, da sie feststehende IP-Adressen benötigen. Selbst-signierte Zertifikate oder Zertifikate von einer PKI ermöglichen mobilen Systemen jedoch die Kommunikation mit einem zentralen Standort.

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

   Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

   ---

2. **Konfigurieren Sie das zentrale System, so dass es mobile Systeme erkennt.**

   a. **Richten Sie die `/etc/hosts`-Datei ein.**

   Das zentrale System muss bestimmte Adressen für mobile Systeme nicht erkennen.

   ```
   # /etc/hosts on central
   central 192.xxx.xxx.x
   ```

   b. **Richten Sie die `ipsecinit.conf`-Datei ein.**

   Das zentrale System benötigt eine Richtlinie, die einen breiten Bereich an IP-Adressen zulässt. Später stellen Zertifikate in der IKE-Richtlinie sicher, dass Systeme, die eine Verbindung herzustellen versuchen, hierzu berechtigt sind.

   ```
   # /etc/inet/ipsecinit.conf on central
   # Keep everyone out unless they use this IPsec policy:
   {} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
   ```

   c. **Richten Sie die `ike.config`-Datei ein.**

   DNS identifiziert das zentrale System. Zur Authentifizierung des Systems werden Zertifikate verwendet.

   ```
   ## /etc/inet/ike/ike.config on central
   # Global parameters
   #
   # Find CRLs by URI, URL, or LDAP
   # Use CRL from organization's URI
   use_http
   #
   # Use web proxy
   proxy "http://somecache.domain:port/"
   #
   # Use LDAP server
   ```

```
ldap_server    "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root    "C=US, O=Domain Org, CN=Domain STATE"
#
# List self-signed certificates - trust server and enumerated others
#cert_trust    "DNS=central.domain.org"
#cert_trust    "DNS=mobile.domain.org"
#cert_trust    "DN=CN=Domain Org STATE (CLASS), O=Domain Org
#cert_trust    "email=root@central.domain.org"
#cert_trust    "email=user1@mobile.domain.org"
#

# Rule for mobile systems with certificate
{
  label "Mobile systems with certificate"
  local_id_type DNS

# Any mobile system who knows my DNS or IP can find me.

  local_id "central.domain.org"
  local_addr 192.xxx.xxx.x

# Root certificate ensures trust,
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

3 Melden Sie sich bei jedem mobilen System an und konfigurieren Sie das System so, dass es das zentrale System findet.

a. Richten Sie die `/etc/hosts`-Datei ein.

Die `/etc/hosts`-Datei benötigt keine Adresse für das mobile System, kann aber eine bereitstellen. Die Datei muss eine öffentliche IP-Adresse für das zentrale System enthalten.

```
# /etc/hosts on mobile
mobile 10.x.x.xx
central 192.xxx.xxx.x
```

b. Richten Sie die `ipsecinit.conf`-Datei ein.

Das mobile System muss das zentrale System über die öffentliche IP-Adresse finden können. Die Systeme müssen mit der gleichen IPsec-Richtlinie konfiguriert sein.

```
# /etc/inet/ipsecinit.conf on mobile
# Find central
{raddr 192.xxx.xxx.x} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

c. Richten Sie die `ike.config`-Datei ein.

Als Bezeichner darf keine IP-Adresse verwendet werden. Für mobile Systeme sind die folgenden Bezeichner gültig:

- `DN=`*ldap-Verzeichnisname*
- `DNS=`*Adresse-des-Domänennamenservers*
- `email=`*E-Mail-Adresse*

Zur Authentifizierung des mobilen Systems werden Zertifikate verwendet.

```
## /etc/inet/ike/ike.config on mobile
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server   "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root    "C=US, O=Domain Org, CN=Domain STATE"
#
# Self-signed certificates - trust me and enumerated others
#cert_trust    "DNS=mobile.domain.org"
#cert_trust    "DNS=central.domain.org"
#cert_trust    "DN=CN=Domain Org STATE (CLASS), O=Domain Org
#cert_trust    "email=user1@domain.org"
#cert_trust    "email=root@central.domain.org"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile with certificate"
    local_id_type DNS

# NAT-T can translate local_addr into any public IP address
# central knows me by my DNS

    local_id "mobile.domain.org"
    local_addr 0.0.0.0/0

# Find central and trust the root certificate
    remote_id "central.domain.org"
    remote_addr 192.xxx.xxx.x

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

4 Lesen Sie die IKE-Konfiguration in den Systemkern ein.

- **Wenn Sie mit mindestens Solaris 10 4/09 arbeiten, aktivieren Sie den `ike`-Service.**

```
# svcadm enable svc:/network/ipsec/ike
```

- **Wenn Sie eine ältere Version als Solaris 10 4/09 verwenden, muss das System neu gestartet werden.**

  ```
  # init 6
  ```

  Alternativ stoppen und starten Sie den `in.iked`-Daemon.

Beispiel 23–8 Konfiguration eines zentralen Computers zum Akzeptieren von IPsec-Verkehr von einem mobilen System

IKE kann Aushandlungen hinter einer NAT-Box initiieren. Das ideale Setup für IKE sieht jedoch keine zwischengeschaltete NAT-Box vor. Im folgenden Beispiel wurden die Root-Zertifikate von einer CA ausgegeben und auf dem mobilen und dem zentralen System eingepflegt. Ein zentrales System akzeptiert IPsec-Aushandlungen von einem System hinter einer NAT-Box. `main1` ist ein Unternehmenssystem, das Verbindungen von Offsite-Systemen akzeptiert. Informationen zum Einrichten von Offsite-Systemen finden Sie in Beispiel 23–9.

```
## /etc/hosts on main1
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server   "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
  label "Off-site system with root certificate"
  local_id_type DNS
  local_id "main1.domain.org"
  local_addr 192.168.0.100

# Root certificate ensures trust,
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5
```

```
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha1}
}
```

Beispiel 23–9 Konfiguration eines Systems hinter einer NAT-Box mit IPsec

Im folgenden Beispiel wurden die Root-Zertifikate von einer CA ausgegeben und auf dem mobilen sowie auf dem zentralen System eingepflegt. `mobile1` stellt von zu Hause aus eine Verbindung mit dem Unternehmenshauptsitz her. Das Internet Service-Providers (ISP)-Netzwerk verwendet eine NAT-Box, damit der ISP `mobile1` eine private Adresse zuordnen kann. Die NAT-Box übersetzt die private Adresse dann in eine öffentliche IP-Adresse, die gemeinsam mit anderen ISP-Netzwerkknoten genutzt wird. Das Hauptbüro des Unternehmens befindet sich nicht hinter einer NAT-Box. Informationen zur Einrichtung des Computers in der Unternehmenszentrale finden Sie unter Beispiel 23–8.

```
## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server   "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
  label "Off-site mobile1 with root certificate"
  local_id_type DNS
  local_id "mobile1.domain.org"
  local_addr 0.0.0.0/0

# Find main1 and trust the root certificate
  remote_id "main1.domain.org"
```

```
  remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Beispiel 23–10 Akzeptieren selbst-signierter Zertifikate von einem mobilen System

Im folgenden Beispiel wurden selbst-signierte Zertifikate ausgegeben, die sich auf dem mobilen und auf dem zentralen System befinden. `main1` ist ein Unternehmenssystem, das Verbindungen von Offsite-Systemen akzeptiert. Wie Sie die Offsite-Systeme einrichten, erfahren Sie in Beispiel 23–11.

```
## /etc/hosts on main1
main1 192.168.0.100


## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}


## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Self-signed certificates - trust me and enumerated others
cert_trust    "DNS=main1.domain.org"
cert_trust    "jdoe@domain.org"
cert_trust    "user2@domain.org"
cert_trust    "user3@domain.org"
#
# Rule for off-site systems with trusted certificate
{
  label "Off-site systems with trusted certificates"
  local_id_type DNS
  local_id "main1.domain.org"
  local_addr 192.168.0.100

# Trust the self-signed certificates
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Beispiel 23–11 Verwenden von selbst-signierten Zertifikaten zum Aufnehmen einer Verbindung mit einem zentralen System

Im folgenden Beispiel versucht `mobile1`, eine Verbindung von zu Hause aus mit dem Hauptbüro des Unternehmens herzustellen. Die Zertifikate wurden ausgegeben und befinden

sich auf dem mobilen und auf dem zentralen System. Das ISP-Netzwerk verwendet eine NAT-Box, damit der ISP `mobile1` eine private Adresse zuordnen kann. Die NAT-Box übersetzt die private Adresse dann in eine öffentliche IP-Adresse, die gemeinsam mit anderen ISP-Netzwerkknoten genutzt wird. Das Hauptbüro des Unternehmens befindet sich nicht hinter einer NAT-Box. Informationen zum Einrichten der Computer am Unternehmenshauptsitz finden Sie in Beispiel 23–10.

```
## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters

# Self-signed certificates - trust me and the central system
cert_trust    "jdoe@domain.org"
cert_trust    "DNS=main1.domain.org"
#
# Rule for off-site systems with trusted certificate
{
  label "Off-site mobile1 with trusted certificate"
  local_id_type email
  local_id "jdoe@domain.org"
  local_addr 0.0.0.0/0

# Find main1 and trust the certificate
  remote_id "main1.domain.org"
  remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Konfiguration von IKE zum Suchen angehängter Hardware (Übersicht der Schritte)

In der folgenden Tabelle wird auf Verfahren verwiesen, in denen beschrieben wird, wie IKE über angehängte Hardware informiert wird. IKE muss über angehängte Hardware informiert sein, bevor IKE die Hardware verwenden kann. Um die Hardware zu verwenden, folgen Sie den Hardware-Verfahren unter „Konfiguration von IKE mit PublicKey-Zertifikaten“ auf Seite 624.

Hinweis – Sie müssen IKE nicht über On-Chip-Hardware informieren. Der UltraSPARC® T2-Prozessor beinhaltet beispielsweise kryptografische Beschleunigung. Sie müssen IKE nicht konfigurieren, damit die On-Chip-Accelerators gefunden werden.

Aufgabe	Beschreibung	Siehe
Übertragen der IKE-Schlüsselvorgänge auf das Sun Crypto Accelerator 1000-Board	Verbinden Sie IKE mit der PKCS&;#11-Bibliothek.	„So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 1000-Board" auf Seite 651
Übertragen der IKE-Schlüsselvorgänge auf das Sun Crypto Accelerator 4000-Board und speichern der Schlüssel auf dem Board	Verbinden Sie IKE mit der PKCS&;#11-Bibliothek und listen Sie die Namen der angehängten Hardware auf.	„So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 4000-Board" auf Seite 652

Konfiguration von IKE zum Suchen angehängter Hardware

Public Key-Zertifikate können auch auf angehängter Hardware gespeichert werden. Das Sun Crypto Accelerator 1000-Board stellt nur Speicherkapazität zur Verfügung. Das Sun Crypto Accelerator 4000- und Sun Crypto Accelerator 6000-Board bietet Speicherkapazität und ermöglicht das Abgeben von Public Key-Vorgängen vom System auf das Board.

▼ So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 1000-Board

Bevor Sie beginnen Bei dem folgenden Verfahren wird davon ausgegangen, dass ein Sun Crypto Accelerator 1000-Board an das System angehängt ist. Außerdem muss die Software für das Board installiert und konfiguriert sein. Anweisungen finden Sie im *Sun Crypto Accelerator 1000 Board Version 2.0 Installation and User's Guide*.

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

---

2. **Prüfen Sie, ob die PKCS&;#11-Bibliothek verlinkt ist.**

   Geben Sie den folgenden Befehl ein, um festzustellen, ob eine PKCS&;#11-Bibliothek verlinkt ist:

```
# ikeadm get stats
Phase 1 SA counts:
Current:   initiator:          0   responder:          0
Total:     initiator:          0   responder:          0
Attempted: initiator:          0   responder:          0
Failed:    initiator:          0   responder:          0
           initiator fails include 0 time-out(s)
PKCS#11 library linked in from /usr/lib/libpkcs11.so
#
```

3. **Solaris 10 1/06: Ab diesem Release können Sie Schlüssel im Softtoken-Schlüsselspeicher speichern.**

   Informationen zum Schlüsselspeicher, der über das Solaris Cryptographic Framework bereitgestellt wird, finden Sie in der Manpage `cryptoadm(1M)` Ein Beispiel zur Verwendung des Schlüsselspeichers finden Sie in Example 23–12.

▼ So konfigurieren Sie IKE zur Suche nach dem Sun Crypto Accelerator 4000-Board

Bevor Sie beginnen

Bei dem folgenden Verfahren wird davon ausgegangen, dass ein Sun Crypto Accelerator 4000-Board an das System angehängt ist. Außerdem muss die Software für das Board installiert und konfiguriert sein. Anweisungen finden Sie im *Sun Crypto Accelerator 4000 Board Version 1.1 Installation and User's Guide*.

Falls Sie ein Sun Crypto Accelerator 6000-Board verwenden, lesen Sie den *Sun Crypto Accelerator 6000 Board Version 1.1 User's Guide* , um Anweisungen zu erhalten.

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

---

2 Prüfen Sie, ob die PKCS&;#11-Bibliothek verlinkt ist.

IKE verarbeitet die Schlüsselerzeugung und -speicherung auf dem Sun Crypto Accelerator 4000-Board mithilfe der Programmroutinen der Bibliothek. Geben Sie den folgenden Befehl ein, um festzustellen, ob eine PKCS&;#11-Bibliothek verlinkt ist:

```
$ ikeadm get stats
...
PKCS#11 library linked in from /usr/lib/libpkcs11.so
$
```

Hinweis – Für RSA unterstützt das Sun Crypto Accelerator 4000-Board Schlüssel bis zu 2048 Bit. Für DSA unterstützt dieses Board Schlüssel bis zu 1024 Bit.

---

3 Suchen Sie die Token-ID für das angehängte Sun Crypto Accelerator 4000-Board.

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":

"Sun Metaslot                    "
```

Die Bibliothek gibt eine Token-ID mit 32 Zeichen zurück. Die Token-ID wird auch als Schlüsselspeichername bezeichnet. In diesem Beispiel können Sie das Token `Sun Metaslot` mit den `ikecert`-Befehlen zum Speichern und Beschleunigen der IKE-Schlüssel verwenden.

Anweisungen zum Arbeiten mit dem Token finden Sie unter „So erzeugen Sie PublicKey-Zertifikate und speichern sie auf angehängter Hardware“ auf Seite 636.

Die einführenden Leerzeichen werden von dem Befehl `ikecert` automatisch aufgefüllt.

Beispiel 23–12 Suchen und Verwenden von Metaslot-Token

Token können auf einem Datenträger, auf einem angehängten Board oder im Softtoken-Schlüsselspeicher des Solaris Encryption Framework gespeichert werden. Die Token-ID des Softtoken-Schlüsselspeichers könnte wie folgt aussehen:

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":

"Sun Metaslot                  "
```

Informationen zum Erstellen eines Passwortsatzes für den Softtoken-Schlüsselspeicher finden Sie in der Manpage `pktool(1)`.

Mit einem Befehl ähnlich dem Folgenden fügen Sie das Zertifikat zum Softtoken-Schlüsselspeicher hinzu. `Sun.Metaslot.cert` ist eine Datei mit dem CA-Zertifikat.

```
# ikecert certdb -a -T "Sun Metaslot" < Sun.Metaslot.cert
Enter PIN for PKCS#11 token:      Type user:passphrase
```

Ändern der IKE-Übertragungsparameter (Übersicht der Schritte)

In der folgenden Tabelle wird auf Verfahren zur Konfiguration der Übertragungsparameter verwiesen.

Aufgabe	Beschreibung	Siehe
Schlüsselaushandlungen effizienter gestalten	Ändern Sie die Parameter zur Schlüsselaushandlung.	„So ändern Sie die Dauer der Phase 1 IKE-Schlüsselaushandlung“ auf Seite 655
Konfiguration der Schlüsselaushandlung, um Verzögerungen bei der Übertragung zu gestatten	Verlängern Sie die Parameter zur Schlüsselaushandlung.	Beispiel 23–13
Konfiguration der Schlüsselaushandlung, so dass sie schnell zum Erfolg führt oder schnell einen Fehler anzeigt	Verkürzen Sie die Parameter zur Schlüsselaushandlung.	Beispiel 23–14

Ändern der IKE-Übertragungsparameter

Wenn IKE Schlüssel aushandelt, wirkt sich die Übertragungsgeschwindigkeit auf den Erfolg der Aushandlung aus. Normalerweise müssen Sie die Standardwerte für die IKE-Übertragungsparameter nicht ändern. Eventuell müssen die Übertragungswerte jedoch geändert werden, um die Schlüsselaushandlung bei extrem frequentierten Leitungen zu optimieren oder um ein Problem zu reproduzieren.

Bei einer längeren Aushandlung kann IKE die Schlüssel aus über unzuverlässige Übertragungsleitungen aushandeln. Sie verlängern bestimmte Parameter, so dass schon die ersten Versuche erfolgreich sind. Wenn der erste Versuch nicht erfolgreich ist, können Sie nachfolgenden Versuchen mehr Zeit gewähren, damit sie erfolgreich abgeschlossen werden.

Bei einer kürzeren Dauer können Sie von den Vorteilen zuverlässiger Übertragungsleitungen profitieren. Sie können schneller einen Wiederholversuch bei fehlgeschlagenen Aushandlungen einleiten, um so die Aushandlung insgesamt zu beschleunigen. Bei der Suche nach der Ursache eines Problems können Sie auch die Aushandlung beschleunigen, um schnell einen Fehler zu erzeugen. Eine kürzere Aushandlung bedeutet auch, dass die Phase 1 SAs über deren gesamte Lebendauer genutzt werden können.

▼ So ändern Sie die Dauer der Phase 1 IKE-Schlüsselaushandlung

1. **Nehmen Sie über die Systemkonsole die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

   Hinweis – Eine remote Anmeldung führt zu sicherheitskritischem Datenverkehr, der abgehört werden könnte. Auch wenn Sie eine remote Anmeldung schützen, wird die Sicherheit des Systems auf die Sicherheit der remoten Anmeldesitzung reduziert. Verwenden Sie den Befehl `ssh`, um sich sicher remote anzumelden.

   ---

2. **Ändern Sie die Standardwerte der globalen Übertragungsparameter auf jedem System.**

   Ändern Sie die Phase 1 Parameter für die Aushandlungsdauer in der Datei `/etc/inet/ike/config` auf jedem System.

```
### ike/config file on      system

## Global parameters
#
## Phase 1 transform defaults
#
#expire_timer      300
#retry_limit         5
#retry_timer_init    0.5 (integer or float)
#retry_timer_max    30   (integer or float)
```

`expire_timer` — Die Zeit in Sekunden, die eine noch nicht abgeschlossene IKE Phase I-Aushandlung weiter ausgeführt werden darf, bis der Aushandlungsversuch gelöscht wird. Standardmäßig werden die Versuche über 30 Sekunden ausgeführt.

`retry_limit` — Die Anzahl an wiederholten Übertragungen, bevor die IKE-Aushandlung abgebrochen wird. Standardmäßig versucht IKE fünf Übertragungen.

`retry_timer_init` — Das Erstintervall zwischen den Übertragungsversuchen. Dieses Intervall wird verdoppelt, bis der Wert von `retry_timer_max` erreicht ist. Das Erstintervall beträgt 0,5 Sekunden.

`retry_timer_max` — Das maximale Intervall zwischen den Übertragungsversuchen. Das Intervall für die Übertragungsversuche wächst bis zu diesem Wert an. Standardmäßig beträgt der Grenzwert 30 Sekunden.

3 Lesen Sie die geänderte Konfiguration in den Systemkern ein.

- **Wenn Sie mindestens mit Solaris 10 4/09 arbeiten, aktualisieren Sie den `ike`-Service.**

  ```
  # svcadm refresh svc:/network/ipsec/ike
  ```

- **Wenn Sie eine ältere Version als Solaris 10 4/09 verwenden, starten Sie das System neu.**

  ```
  # init 6
  ```

  Alternativ stoppen und starten Sie den `in.iked`-Daemon.

Beispiel 23–13 Verlängern der IKE Phase 1-Aushandlungszeiten

Im folgenden Beispiel ist ein System über eine stark frequentierte Übertragungsleitung mit seinem Peer verbunden. Die ursprünglichen Einstellungen in der Datei sind mit Kommentarzeichen versehen. Die neuen Einstellungen verlängern die Aushandlungszeit.

```
### ike/config file on partym
## Global Parameters
#
## Phase 1 transform defaults
#expire_timer   300
#retry_limit      5
#retry_timer_init 0.5 (integer or float)
#retry_timer_max 30   (integer or float)
#
expire_timer  600
retry_limit  10
retry_timer_init  2.5
retry_timer_max  180
```

Beispiel 23–14 Verkürzen der IKE Phase 1-Aushandlungszeiten

Im folgenden Beispiel ist ein System über eine Hochgeschwindigkeitsleitung mit wenig Verkehr mit seinem Peer verbunden. Die ursprünglichen Einstellungen in der Datei sind mit Kommentarzeichen versehen. Die neuen Einstellungen verkürzen die Aushandlungszeit.

```
### ike/config file on partym
## Global Parameters
#
## Phase 1 transform defaults
#expire_timer   300
#retry_limit      5
#retry_timer_init 0.5 (integer or float)
#retry_timer_max 30   (integer or float)
#
expire_timer  120
retry_timer_init  0.20
```

KAPITEL 24

Internet Key Exchange (Referenz)

Dieses Kapitel enthält die folgenden Referenzinformationen zum IKE:

- „IKE Service Management Facility“ auf Seite 657
- „IKE-Daemon“ auf Seite 658
- „IKE-Richtliniendatei“ auf Seite 658
- „IKE-Verwaltungsbefehl“ auf Seite 659
- „IKE PresharedKeys-Dateien“ auf Seite 660
- „IKE PublicKey-Datenbanken und -Befehle“ auf Seite 660

Informationen zur Implementierung von IKE finden Sie in Kapitel 23, „Konfiguration von IKE (Aufgaben)“. Eine Einführung in IKE finden Sie in Kapitel 22, „Internet Key Exchange (Übersicht)“.

IKE Service Management Facility

`svc:/network/ipsec/ike:default` **-Service –** Die Service Management Facility (SMF) stellt zur IKE-Verwaltung den `ike`-Service zur Verfügung. Dieser Service ist standardmäßig deaktiviert. Vor der Aktivierung dieses Service müssen Sie eine IKE-Konfigurationsdatei (`/etc/inet/ike/config`) erstellen.

Die folgenden Eigenschaften des `ike`-Service können konfiguriert werden:

- `config_file`-**Eigenschaft:** Der Speicherort der IKE-Konfigurationsdatei. Der anfängliche Wert lautet `/etc/inet/ike/config`.
- `debug level`-**Eigenschaft:** Die Fehlersuchebene des `in.iked`-Daemons. Der anfängliche Wert lautet `op` (operational; betriebsbereit). Weitere mögliche Werte finden Sie in der Tabelle mit dem Fehlersuchwerten unter *Object Types* in der Manpage `ikeadm`(1M).
- `admin_privilege`-**Eigenschaft:** Die Privilegstufe des `in.iked`-Daemons. Der anfängliche Wert lautet `base`. Sonstige mögliche Werte sind `modkeys` und `keymat`. Details finden Sie unter „IKE-Verwaltungsbefehl“ auf Seite 659.

Weitere Informationen zur SMF finden Sie in Kapitel 18, „Managing Services (Overview)" in *System Administration Guide: Basic Administration*. Lesen Sie hierzu auch die Manpages `smf(5)`, `svcadm(1M)` und `svccfg(1M)`.

IKE-Daemon

Der `in.iked`-Daemon automatisiert die Verwaltung der kryptografischen Schlüssel für IPsec auf einem Solaris-System. Der Daemon führt die Aushandlung mit einem remoten System aus, auf dem das gleiche Protokoll ausgeführt wird, um auf sichere Weise authentifiziertes Schlüsselmaterial für Sicherheitszuordnungen (SAs) bereitzustellen. Der Daemon muss auf allen Systemen ausgeführt werden, die sicher miteinander kommunizieren sollen.

Standardmäßig ist der `svc:/network/ipsec/ike:default`-Service nicht aktiviert. Nach der Konfiguration der `/etc/inet/ike/config`-Datei und der Aktivierung des `ike`-Service wird der `in.iked`-Daemon beim Booten des Systems ausgeführt.

Wenn der IKE-Daemon ausgeführt wird, authentifiziert sich das System gegenüber seiner IKE-Peer-Entität in der Phase 1 Exchange. Der Peer ist, ebenso wie die zu verwendenden Authentifizierungsmethoden, in der IKE-Richtliniendatei definiert. Als Nächstes richtet der Daemon dann die Schlüssel für den Phase 2 Exchange ein. Die IKE-Schlüssel werden in einem in der Richtliniendatei festgelegten Intervall automatisch aktualisiert. Der `in.iked`-Daemon empfängt eingehende IKE-Anforderungen aus dem Netzwerk und Anforderungen nach abgehendem Verkehr über den `PF_KEY`-Socket. Weitere Informationen finden Sie in der Manpage `pf_key(7P)`.

Der IKE-Daemon unterstützt zwei Befehle. Der `ikeadm`-Befehl kann zur Anzeige und vorübergehenden Änderung der IKE-Richtlinie verwendet werden. Wenn Sie die IKE-Richtlinie dauerhaft ändern möchten, müssen Sie die Eigenschaften des `ike`-Service bearbeiten. Die Verfahrensweise wird unter „So rufen Sie IKE PresharedKeys auf" auf Seite 618 erläutert.

Mit dem Befehl `ikecert` können Sie die PublicKey-Datenbanken anzeigen und pflegen. Dieser Befehl dient zum Verwalten der lokalen Datenbanken `ike.privatekeys` und `publickeys` . Darüber hinaus werden mit diesem Befehl die PublicKey-Vorgänge durchgeführt und die PublicKeys auf der angehängten Hardware gespeichert.

IKE-Richtliniendatei

Die Konfigurationsdatei für die IKE-Richtlinie, `/etc/inet/ike/config`, verwaltet die Schlüssel für die Schnittstellen, die in der IPsec-Richtliniendatei, `/etc/inet/ipsecinit.conf`, geschützt sind. Die IKE-Richtliniendatei verwaltet die Schlüssel für IKE und für die IPsec SAs. Der IKE-Daemon selbst erfordert Schlüsselmaterial in Phase 1 Exchange.

Das Schlüsselmanagement mit IKE baut auf Regeln und globale Parameter. Eine IKE-Regel identifiziert die Systeme oder Netzwerke, die das Schlüsselmaterial sichert, und gibt die

Authentifizierungsmethode an. Globale Parameter enthalten Objekte wie den Pfad zu einem angehängten Hardwarebeschleuniger. Beispiele für IKE-Richtliniendateien finden Sie unter „Konfiguration von IKE mit PresharedKeys (Übersicht der Schritte)“ auf Seite 612. Beispiele und Beschreibungen der IKE-Richtlinieneinträge finden Sie in der Manpage `ike.config(4)`.

Die von IKE unterstützten IPsec SAs schützen die IP-Datagramme gemäß den Richtlinien, die in der Konfigurationsdatei für die IPsec-Richtlinie, `/etc/inet/ipsecinit.conf`, aufgestellt wurden. Die IKE-Richtliniendatei legt fest, ob Perfect Forward Security (PFS) beim Erstellen der IPsec SAs verwendet werden soll.

Die Datei `ike/config` kann den Pfad zu einer Bibliothek enthalten, die gemäß dem Standard RSA Security Inc. PKCS&;#11 Cryptographic Token Interface (Cryptoki) implementiert wird. IKE verwendet diese PKCS&;#11-Bibliothek für den Zugriff auf Hardware zur Schlüsselbeschleunigung und -speicherung.

Die Sicherheitsaspekte für die `ike/config`-Datei entsprechend denen für die `ipsecinit.conf`-Datei. Ausführliche Informationen finden Sie im Abschnitt „Sicherheitsbetrachtungen für `ipsecinit.conf` und `ipsecconf`“ auf Seite 596.

IKE-Verwaltungsbefehl

Mit dem `ikeadm`-Befehl können Sie Folgendes auszuführen:

- Aspekte des IKE-Daemon-Prozesses anzeigen.
- Parameter ändern, die an den IKE-Daemon übergeben werden.
- Statistiken zur SA-Erstellung während der Phase 1 Exchange anzeigen.
- IKE-Prozesse debuggen.
- Aspekte des IKE-Status anzeigen.
- Ändern Sie die Konfiguration des IKE-Daemon.
- Statistiken zur SA-Erstellung während der Phase 1 Exchange anzeigen.
- IKE-Protokollaustausch debuggen.

Beispiele und eine vollständige Beschreibung der Optionen dieses Befehls finden Sie in der Manpage `ikeadm(1M)`

Je nach Privilegstufe des ausgeführten IKE-Daemons können verschiedene Aspekte des Daemons angezeigt und geändert werden. Es werden drei Privilegstufen unterschieden.

`base`-Stufe — Sie können das Schlüsselmaterial weder anzeigen noch ändern. `Base` ist die Standard-Privilegstufe.

`modkeys`-Stufe — Sie können PresharedKeys entfernen, ändern und hinzufügen.

`keymat`-Stufe — Sie können das tatsächliche Schlüsselmaterial mit dem Befehl `ikeadm` anzeigen.

Wenn Sie die Privilegstufe nur vorübergehend ändern möchten, können Sie den `ikeadm`-Befehl verwenden. Wenn die Änderung dauerhaft erfolgen soll, ändern Sie die `admin_privilege`-Eigenschaft des `ike`-Service. Die Verfahrensweise wird unter „Verwalten von IKE- und IPsec-Services“ auf Seite 553.

Die Sicherheitsaspekte für den `ikeadm`-Befehl entsprechen denen für den `ipseckey`-Befehl. Ausführliche Informationen finden Sie unter „Sicherheitsbetrachtungen für `ipseckey`“ auf Seite 598.

IKE PresharedKeys-Dateien

Wenn Sie PresharedKeys manuell erstellen, werden die Schlüssel in Dateien im Verzeichnis `/etc/inet/secret` gespeichert. Die Datei `ike.preshared` enthält die PresharedKeys für die Internet Security Association and Key Management Protocol (ISAKMP) SAs. Die Datei `ipseckeys` enthält die PresharedKeys für die IPsec SAs. Die Dateien sind mit `0600` geschützt. Das Verzeichnis `secret` ist mit `0700` geschützt.

- Sie erstellen eine `ike.preshared`-Datei, wenn Sie die `ike/config`-Datei so konfigurieren, dass sie PresharedKeys erfordert. Sie geben das Schlüsselmaterial für die ISAKMP SAs, das heißt, für die IKE-Authentifizierung, in die Datei `ike.preshared` ein. Da die PresharedKeys zur Authentifizierung der Phase 1 Exchange verwendet werden, muss die Datei schon gültig sein, bevor der `in.iked`-Daemon gestartet wird.
- Die `ipseckeys`-Datei enthält das Schlüsselmaterial für die IPsec SAs. Beispiele zur manuellen Verwaltung der Datei finden Sie unter „So erstellen Sie manuell IPsec-Sicherheitszuordnungen“ auf Seite 545. Diese Datei wird vom IKE-Daemon nicht verwendet. Das Schlüsselmaterial, das IKE für die IPsec SAs erzeugt, wird im Kernel gespeichert.

Hinweis – PresharedKeys können die Vorteile der Hardware-Speicherung nicht nutzen. PresharedKeys werden vom System erzeugt und im System gespeichert.

IKE PublicKey-Datenbanken und -Befehle

Mit dem Befehl `ikecert` können Sie die PublicKey-Datenbanken des lokalen Systems bearbeiten. Sie verwenden diesen Befehl, wenn die Datei `ike/config` PublicKey-Zertifikate erfordert. Da IKE diese Datenbanken zur Authentifizierung der Phase 1 Exchange benötigt, müssen sie schon gefüllt sein, bevor der `in.iked`-Daemon aktiviert wird. Jede der drei Datenbanken verarbeitet drei Unterbefehle: `certlocal`, `certdb` und `certrldb`.

Mit dem Befehl `ikecert` wird auch die Schlüsselspeicherung verwaltet. Schlüssel können auf einem Datenträger, auf einem angehängten Sun Crypto Accelerator 6000- oder Sun Crypto

Accelerator 4000-Board oder in einem Softtoken-Schlüsselspeicher gespeichert werden. Der Softtoken-Schlüsselspeicher ist verfügbar, wenn der Metaslot im Solaris Cryptographic Framework zur Kommunikation mit dem Hardware-Gerät verwendet wird. Der Befehl `ikecert` verwendet die PKCS&;#11-Bibliothek zum Lokalisieren des Schlüsselspeichers.

- **Solaris 10 1/06**: Ab diesem Release wird muss die Bibliothek nicht mehr angegeben werden. Standardmäßig befindet sich die PKCS&;#11-Bibliothek unter `/usr/lib/libpkcs11.so`.
- **Solaris 10**: In diesem Release muss der PKCS&;#11 -Eintrag vorhanden sein. Andernfalls funktioniert die Option `-T` des Befehls `ikecert` nicht. Der Eintrag muss dem Folgenden ähneln:

```
pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

Weitere Informationen finden Sie in der Manpage `ikecert`(1M) Informationen zum Metaslot und dem Softtoken-Schlüsselspeicher finden Sie in der Manpage `cryptoadm`(1M).

`ikecert tokens`-Befehl

Das Argument `Tokens` führt die verfügbaren Token-IDs auf. Mit Token-IDs können die Befehle `ikecert certlocal` und `ikecert certdb` PublicKey-Zertifikate und Zertifikat-Anforderungen erstellen. Die Zertifikate und Zertifikat-Anforderungen werden vom Cryptographic Framework im Softtoken-Schlüsselspeicher oder auf dem angehängten Sun Crypto Accelerator 6000- oder Sun Crypto Accelerator 4000-Board gespeichert. Der Befehl `ikecert` verwendet die PKCS&;#11-Bibliothek zum Lokalisieren des Schlüsselspeichers.

`ikecert certlocal`-Befehl

Mit dem Unterbefehl `certlocal` wird die PrivateKey-Datenbanken verwaltet. Mit den Optionen dieses Unterbefehl können Sie PrivateKeys hinzufügen, anzeigen und entfernen. Mit diesem Unterbefehl wird auch entweder ein selbst-signiertes Zertifikat oder eine Zertifikat-Anforderung erstellt. Die Option `-ks` erstellt ein selbst-signiertes Zertifikat. Die Option `-kc` erstellt eine Zertifikat-Anforderung. Die Schlüssel werden auf dem System im Verzeichnis `/etc/inet/secret/ike.privatekeys` oder mit der Option `-T` auf der angehängten Hardware gespeichert.

Wenn Sie einen PrivateKey erstellen, müssen die Optionen für den Befehl `ikecert certlocal` entsprechende Einträge in der Datei `ike/config` aufweisen. Die Entsprechungen zwischen den `ikecert`-Optionen und den `ike/config`-Einträgen sind in der folgenden Tabelle aufgeführt.

TABELLE 24–1 Entsprechungen zwischen `ikecert`-Optionen und`ike/config`-Einträgen

`ikecert`-**Option**	`ike/config`-**Eintrag**	**Beschreibung**
`-A` *Subjekt-Alternativname*	`cert_trust` *Subjekt-Alternativname*	Ein Alias, der das Zertifikat eindeutig identifiziert. Mögliche Werte sind eine IP-Adresse, eine E-Mail-Adresse oder ein Domänenname.
`-D` *X.509-Distinguished-Name*	*X.509-Distinguished-Name*	Der vollständige Name der Zertifikatsautorität, der das Land (C), den Namen der Organisation (ON), die Organisationseinheit (OU) und den allgemeinen Namen (CN) enthält.
`-t dsa-sha1`	`auth_method dss_sig`	Eine Authentifizierungsmethode, die etwas langsamer als RSA ist.
`-t rsa-md5` und `-t rsa-sha1`	`auth_method rsa_sig`	Eine Authentifizierungsmethode, die etwas schneller als DSA ist. Ein RSA-PublicKey muss groß genug sein, um die größte Nutzlast zu verschlüsseln. In der Regel ist eine Identität, zum Beispiel der X.509 Distinguished Name, die größte Nutzlast.
`-t rsa-md5` und `-t rsa-sha1`	`auth_method rsa_encrypt`	Die RSA-Verschlüsselung verbirgt Identitäten in IKE vor möglichen Mithörern, erfordert aber, dass IKE-Peers die PublicKeys des jeweils anderen Peers kennen.
`-T`	`pkcs11_path`	Die PKCS #11-Bibliothek sorgt für Schlüsselbeschleunigung auf dem Sun Crypto Accelerator 1000-, Sun Crypto Accelerator 6000- und dem Sun Crypto Accelerator 4000-Board. Die Bibliothek stellt auch die Tokens zur Verfügung, die für die Schlüsselspeicherung auf den Sun Crypto Accelerator 6000- und Sun Crypto Accelerator 4000-Boards zuständig sind.

Wenn Sie mit dem Befehl `ikecert certlocal -kc` eine Zertifikat-Anforderung ausgeben, senden Sie die Ausgabe des Befehls an eine PKI-Organisation oder an eine Zertifikatsautorität (CA). Falls Ihr Unternehmen eine eigene PKI ausführt, senden Sie die Ausgabe des Befehls an Ihren PKI-Administrator. Die Zertifikate werden dann von der PKI-Organisation, der CA oder dem PKI-Administrator erstellt. Die von der PKI oder der CA zurückgegebenen Zertifikate dienen als Eingabe für den Unterbefehl `certdb.` Die von der PKI zurückgegebene Zertifikat-Rücknahmeliste (CRL) dient als Eingabe für den Unterbefehl `certrldb`.

`ikecert certdb`-Befehl

Mit dem Unterbefehl `certdb` wird die PublicKey-Datenbank verwaltet. Mit den Optionen dieses Unterbefehl zu können Sie Zertifikate und PublicKeys hinzufügen, anzeigen oder entfernen. Der Befehl akzeptiert Zertifikate, die mit dem Befehl `ikecert certlocal -ks` auf einem remoten System erzeugt wurden, als Eingabe. Verfahren hierzu finden Sie unter „So

konfigurieren Sie IKE mit selbst-signierten PublicKey-Zertifikaten“ auf Seite 625. Darüber hinaus akzeptiert dieser Befehl ein Zertifikat als Eingabe, das Sie von einer PKI oder CA empfangen haben. Informationen hierzu finden Sie unter „So konfigurieren Sie IKE mit Zertifikaten, die von einer CA signiert wurden“ auf Seite 631.

Die Zertifikate und PublicKeys werden im Verzeichnis `/etc/inet/ike/publickeys` auf dem System gespeichert. Mit der Option `-T` werden die Zertifikate, PublicKeys und PrivateKeys auf der angehängten Hardware gespeichert.

`ikecert certrldb`-Befehl

Mit dem Unterbefehl `certrldb` wird die Datenbank der Zertifikat-Rücknahmeliste (CRL), `/etc/inet/ike/crls`, verwaltet. In der CRL-Datenbank werden die Rücknahmelisten für PublicKeys gepflegt. Hierbei handelt es sich um nicht mehr gültige Zertifikate. Wenn PKIs Ihnen eine CRL bereitstellt, können Sie sie mit dem Befehl `ikecert certrldb` in der CRL-Datenbank installieren. Verfahren hierzu finden Sie unter „So verarbeiten Sie eine Zertifikat-Rücknahmeliste“ auf Seite 640.

`/etc/inet/ike/publickeys`-Verzeichnis

Das `/etc/inet/ike/publickeys`-Verzeichnis enthält den öffentlichen Teil eines Paares aus Public und Private Key und dessen Zertifikat in Dateien oder *Slots*. Das Verzeichnis ist mit `0755` geschützt. Es wird mit dem Befehl `ikecert certdb` gefüllt. Mit dem Befehl `-T` werden die Schlüssel auf dem Sun Crypto Accelerator 6000- oder dem Sun Crypto Accelerator 4000-Board anstatt im `publickeys`-Verzeichnis gespeichert.

Die Slots enthalten den X.509 Distinguished Name eines von einem anderen System erzeugten Zertifikates in verschlüsselter Form. Wenn Sie selbst-signierte Zertifikate einsetzen, verwenden Sie das Zertifikat, das Sie vom Administrator des remoten Systems empfangen haben, als Eingabe für den Befehl. Wenn Sie Zertifikate von einer Zertifizierungsstelle verwenden, müssen Sie in dieser Datenbank zwei von der Zertifizierungsstelle signierte Zertifikate installieren. Sie installieren ein Zertifikat, dass auf der zur Zertifizierungsstelle gesendeten Zertifikatssignieranforderung basiert. Sie müssen auch das Zertifikat der Zertifizierungsstelle installieren.

`/etc/inet/secret/ike.privatekeys`-Verzeichnis

Das Verzeichnis `/etc/inet/secret/ike.privatekeys` enthält die PrivateKey-Dateien (Teil des PublicKey-PrivateKey-Paares), die das Schlüsselmaterial für die ISAKMP SAs darstellen. Das Verzeichnis ist mit `0700` geschützt. Das Verzeichnis `ike.privatekeys` wird mit dem Befehl `ikecert certlocal` gefüllt. PrivateKeys werden erst dann wirksam, wenn ihre PublicKey-Pendants, selbst-signierte Zertifikate oder CAs installiert sind. Die

PublicKey-Pendants sind im Verzeichnis `/etc/inet/ike/publickeys` oder auf einem Sun Crypto Accelerator 6000- bzw. einem &sca 4;-Board gespeichert.

`/etc/inet/ike/crls`-Verzeichnis

Das Verzeichnis `/etc/inet/ike/crls` enthält die Dateien der Zertifikat-Rücknahmeliste (CRL). Jede Datei entspricht einer öffentlichen Zertifikatsdatei im Verzeichnis `/etc/inet/ike/publickeys.` PKI-Organisationen stellen die CRLs für ihre Zertifikate bereit. Mit dem Befehl `ikecert certrldb` können Sie die Datenbank füllen.

KAPITEL 25

Oracle Solaris IP Filter (Übersicht)

Dieses Kapitel enthält eine Einführung in Oracle Solaris IP Filter. Aufgaben zu Oracle Solaris IP Filter finden Sie in Kapitel 26, „Oracle Solaris IP Filter (Aufgaben)“.

Dieses Kapitel enthält die folgenden Informationen:

- „Neuerungen bei Oracle Solaris IP Filter“ auf Seite 665
- „Einführung in Oracle Solaris IP Filter“ auf Seite 666
- „Paketverarbeitung mit Oracle Solaris IP Filter“ auf Seite 667
- „Richtlinien zur Verwendung von OpenSolaris IP Filter“ auf Seite 670
- „Verwenden der Oracle Solaris IP Filter-Konfigurationsdateien“ auf Seite 670
- „Arbeiten mit Oracle Solaris IP Filter-Regellisten“ auf Seite 671
- „Paket Filter-Hooks“ auf Seite 677
- „Oracle Solaris IP Filter und das `pfil` STREAMS-Modul“ auf Seite 677
- „IPv6 für Oracle Solaris IP Filter“ auf Seite 678
- „Oracle Solaris IP Filter – Manpages“ auf Seite 679

Neuerungen bei Oracle Solaris IP Filter

In diesem Abschnitt werden die neuen Funktionen von Oracle Solaris IP Filter beschrieben.

Eine vollständige Liste der neuen Funktionen in sowie eine Beschreibung der Solaris-Releases finden Sie im Handbuch *Neuerungen in Oracle Solaris 9 10/10*

Paket Filter-Hooks

Version Solaris 10 7/07: Für die Paketfilterung in Oracle Solaris werden jetzt Paket Filter-Hooks eingesetzt. Diese Funktion bietet Systemadministratoren die folgenden Vorteile:

- Paket Filter-Hooks vereinfachen die Konfiguration von Oracle Solaris IP Filter.
- Die zonenübergreifende Filterung von Paketen wird unterstützt.

- Das Verwenden von Filter-Hooks verbessert die Leistung von Oracle Solaris IP Filter.

Weitere Informationen zu diesen Hooks finden Sie unter „Paket Filter-Hooks“ auf Seite 677. Aufgaben im Zusammenhang mit Paket Filter-Hooks finden Sie in Kapitel 26, „Oracle Solaris IP Filter (Aufgaben)“.

IPv6-Paketfilterung für Oracle Solaris IP Filter

Solaris 10 6/06: Für Administratoren, die einen Teil oder ihre gesamte Netzwerkinfrastruktur mit IPv6 konfigurieren, wurde Oracle Solaris IP Filter aufgewertet. IP Filter unterstützt jetzt auch die IPv6-Paketfilterung. Die IPv6-Paketfilterung kann basierend auf der Quell- oder Ziel-IPv6-Adresse, auf IPv6-Adresspools sowie auf IPv6-Extension-Header erfolgen.

Die Befehle `ipf` und `ipfstat` wurden um die Option `-6` erweitert, so dass sie mit IPv6 verwendet werden können. Obwohl keine Änderungen an der Befehlszeilenschnittstelle für die Befehle `ipmon` und `ippool` vorgenommen wurden, unterstützen auch diese Befehle IPv6. Der Befehl `ipmon` wurde aufgewertet, so dass eine Protokollierung von IPv6-Paketen möglich ist, und der Befehl `ippool` unterstützt die Aufnahme von IPv6-Adressen in Pools.

Weitere Informationen zu IPv6 finden Sie unter ?IPv6 für Oracle Solaris IP Filter“. Aufgaben im Zusammenhang mit der IPv6-Paketfilterung finden Sie in Kapitel 26, „Oracle Solaris IP Filter (Aufgaben)“.

Einführung in Oracle Solaris IP Filter

Oracle Solaris IP Filter ersetzt die SunScreen-Firewall als Firewall-Software für Oracle Solaris. Im Gegensatz zur SunScreen-Firewall bietet Oracle Solaris IP Filter die statusbehaftete Paketfilterung und Network Address Translation (NAT). Darüber hinaus bietet Oracle Solaris IP Filter eine statusfreie Paketfilterung sowie die Möglichkeit, Adresspools zu erstellen und zu verwalten.

Die Paketfilterung bietet allgemeinen Schutz gegen netzwerkbasierte Angriffe. Oracle Solaris IP Filter kann nach IP-Adresse, Port, Protokoll, Netzwerkschnittstelle und Netzverkehrsrichtung filtern. Darüber hinaus kann Oracle Solaris IP Filter nach einer bestimmten IP-Quelladresse, einer IP-Zieladresse, nach einem Bereich von IP-Adressen oder nach Adresspools filtern.

Oracle Solaris IP Filter ist von der Open Source IP Filter-Software abgeleitet. Der Standardpfad zu Anzeige der Lizenzbedingungen, Attribution und den Hinweisen zum Copyright für Open Source IP Filter lautet `/usr/lib/ipf/IPFILTER.LICENCE`. Falls Oracle Solaris nicht unter dem Standardpfad installiert wurde, ändern Sie den angegebenen Pfad so, dass Sie auf die Datei im Installationsverzeichnis zugreifen können.

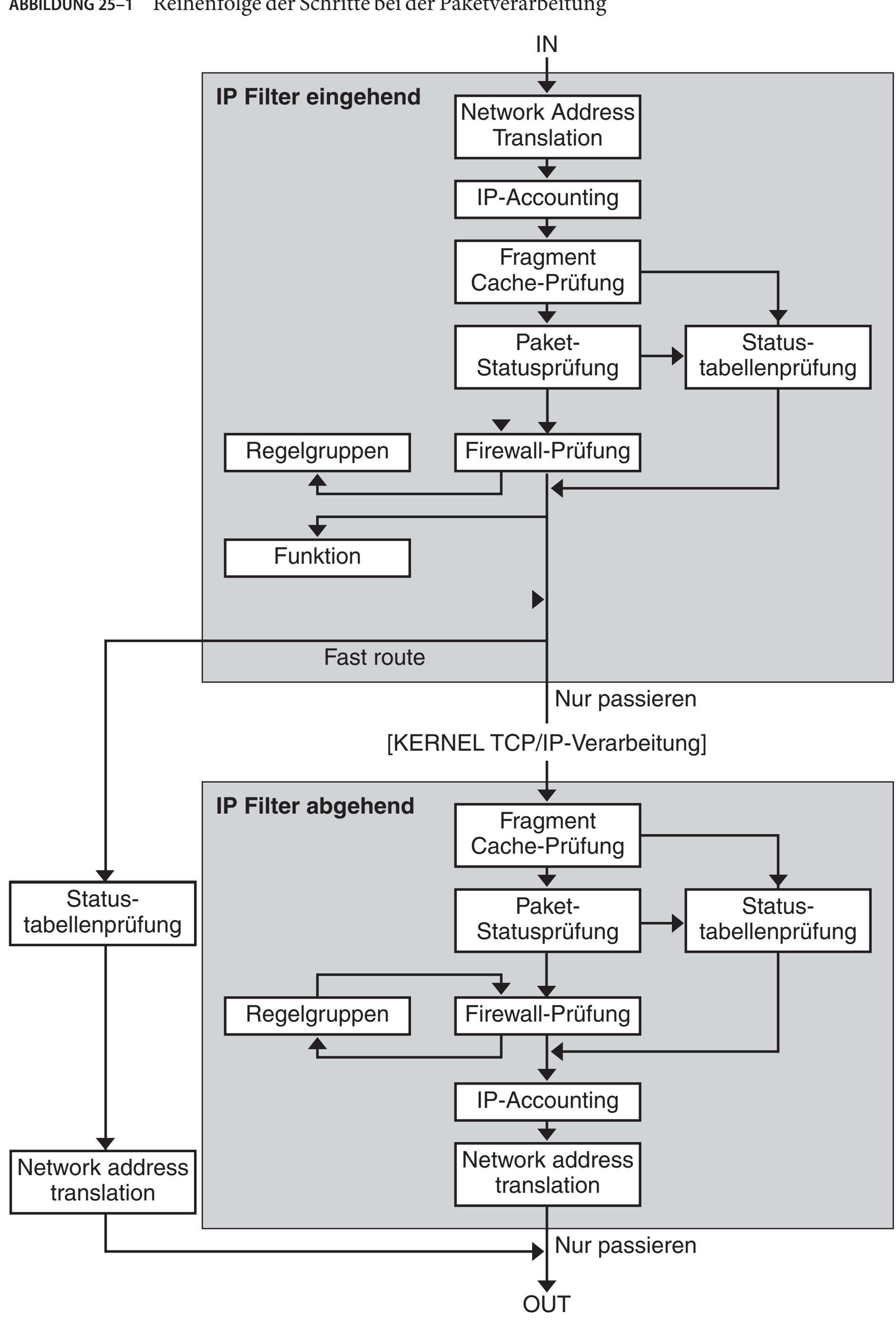
Informationsquellen für Open Source IP Filter

Die Homepage für die Open Source-Software IP Filter von Darren Reed befindet sich unter `http://coombs.anu.edu.au/~avalon/ip-filter.html`. Diese Site enthält Informationen zu Open Source IP Filter, einschließlich einem Link zu einem Lernprogramm mit der Bezeichnung „IP Filter Based Firewalls HOWTO“ (Brendan Conoboy and Erik Fichtner, 2002). Dieses Lernprogramm enthält schrittweise Anleitungen zum Erstellen von Firewalls in einer BSD UNIX-Umgebung. Obwohl es für eine BSD UNIX-Umgebung geschrieben wurde, gilt das Lernprogramm auch für die Konfiguration von Oracle Solaris IP Filter.

Paketverarbeitung mit Oracle Solaris IP Filter

Oracle Solaris IP Filter führt bei der Verarbeitung eines Pakets eine bestimmte Abfolge von Schritten aus. Das folgende Diagramm zeigt die Schritte bei der Paketverarbeitung und die Integration der Filterung in den TCP/IP-Protokollstapel.

ABBILDUNG 25–1 Reihenfolge der Schritte bei der Paketverarbeitung



Die Reihenfolge bei der Paketverarbeitung umfasst:

- **Network Address Translation (NAT)**

  Die Übersetzung einer privaten IP-Adresse in eine andere öffentliche Adresse oder das Aliasing mehrerer privater Adressen mit einer einzigen öffentlichen Adresse. Mit NAT kann ein Unternehmen das Problem mit dem Mangel an IP-Adressen lösen, wenn es vorhandene Netzwerke besitzt und auf das Internet zugreifen muss.

- **IP-Accounting**

  Eingangs- und Ausgangsregeln können getrennt aufgestellt werden und die Anzahl der passierenden Byte aufzeichnen. Jedes Mal, wenn eine Regelübereinstimmung auftritt, werden die Anzahl der Byte im Paket zur Regel hinzugefügt. Auf diese Weise ist das Erstellen von kaskadierenden Statistiken möglich.

- **Fragment Cache-Prüfung**

  Wenn das nächste Paket des aktuellen Datenverkehrs ein Fragment ist und das vorherige Paket zugelassen wurde, wird auch das Paketfragment zugelassen. Dabei werden die Statustabelle und die Regelüberprüfung übergangen.

- **Paket-Statusprüfung**

  Wenn `keep state` (Status beibehalten) in einer Regel enthalten ist, werden alle Pakete in einer bestimmten Sitzung automatisch entweder zugelassen oder blockiert, je nachdem, ob die Regel `pass` oder `block` angibt.

- **Firewall-Prüfung**

  Eingangs- und Ausgangsregeln können getrennt aufgestellt werden und legen fest, ob ein Paket über Solaris IP Filter an die TCP/IP-Routinen oder weiter in das Netzwerk passieren darf.

- **Gruppen**

  Mit Gruppen können Sie Ihre eigene Regelliste in einer Baumstruktur erstellen.

- **Funktion**

  Eine Funktion ist eine durchzuführende Maßnahme. Mögliche Funktionen sind `block`, `pass`, `literal` und `send ICMP response`.

- **Fast-route**

  Fast-route teilt Solaris IP Filter mit, die Pakete nicht in den UNIX IP-Stapel zum Routing passieren zu lassen, was zu einer TTL-Verminderung führt.

- **IP-Authentifizierung**

  Bereits authentifizierte Pakete dürfen Firewall-Schleifen nur einmal passieren, um eine doppelte Verarbeitung zu verhindern.

Richtlinien zur Verwendung von OpenSolaris IP Filter

- OpenSolaris IP Filter wird von den SMF-Services verwaltet: svc:/network/pfil und svc:/network/ipfilter. Eine vollständige Übersicht zur SMF finden Sie in Kapitel 18, „Managing Services (Overview)“ in *System Administration Guide: Basic Administration*. Informationen zu den schrittweisen Verfahren, die der SMF zugeordnet sind, finden Sie in Kapitel 19, „Managing Services (Tasks)“ in *System Administration Guide: Basic Administration*.
- Bei OpenSolaris IP Filter müssen die Konfigurationsdateien direkt bearbeitet werden.
- OpenSolaris IP Filter wird als Teil von Solaris installiert. Standardmäßig wird OpenSolaris IP Filter nach einer Neuinstallation nicht aktiviert. Um die Filterung zu aktivieren, müssen Sie die Konfigurationsdateien bearbeiten und OpenSolaris IP Filter manuell aktivieren. Aktivieren Sie dann die Filterung, indem Sie entweder das System neu booten oder indem Sie die Schnittstellen mit dem Befehl `ifconfig` plumben (aktivieren). Weitere Informationen finden Sie in der Manpage `ifconfig(1M)` Aufgaben im Zusammenhang mit der Aktivierung von OpenSolaris IP Filter finden Sie unter „Konfiguration von Oracle Solaris IP Filter“ auf Seite 681.
- Zur Verwaltung von OpenSolaris IP Filter müssen Sie eine Rolle annehmen, die das IP Filter Management-Rechteprofil umfasst, oder sich als Superuser anmelden. Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .
- IP Network Multipathing (IPMP) unterstützt nur die statusfreie Filterung.
- Sun Cluster-Konfigurationen unterstützen die Filterung mit OpenSolaris IP Filter nicht.
- Eine Filterung zwischen Zonen wird derzeit von OpenSolaris IP Filter nicht unterstützt.

Verwenden der Oracle Solaris IP Filter-Konfigurationsdateien

Oracle Solaris IP Filter kann entweder Firewall-Services oder Network Address Translation (NAT) bereitstellen. Oracle Solaris IP Filter kann mithilfe von ladefähigen Konfigurationsdateien implementiert werden. Oracle Solaris IP Filter enthält ein Verzeichnis namens `/etc/ipf`. Im Verzeichnis `/etc/ipf` können Sie die Konfigurationsdateien `ipf.conf`, `ipnat.conf` und `ippool.conf` erstellen und speichern. Diese Dateien werden während des Bootens automatisch geladen, wenn sie sich im Verzeichnis `/etc/ipf` befinden. Sie können die Konfigurationsdateien auch in einem anderen Verzeichnis speichern und dann manuell laden. Beispiele für die Konfigurationsdateien finden Sie unter „Erstellen und Bearbeiten von Konfigurationsdateien für Oracle Solaris IP Filter“ auf Seite 714.

Arbeiten mit Oracle Solaris IP Filter-Regellisten

Bei der Verwaltung Ihrer Firewall verwenden Sie Oracle Solaris IP Filter, um Regellisten anzugeben, mit denen Ihr Netzwerkverkehr gefiltert wird. Sie können die folgenden Regellistentypen erstellen:

- Paketfilter-Regellisten
- Regellisten für Network Address Translation (NAT)

Darüber hinaus können Sie Adresspools erstellen, um auf IP-Adressgruppen zu verweisen. Diese Pools können Sie dann später in einer Regelliste verwenden. Die Adresspools helfen Ihnen dabei, die Regelverarbeitung zu beschleunigen. Mit Adresspools lassen sich auch große Adressengruppen einfacher verwalten.

Verwenden der Paketfilter-Funktionen in Oracle Solaris IP Filter

Eine Paketfilterung wird mithilfe der Paketfilter-Regellisten eingerichtet. Zum Arbeiten mit Paketfilter-Regellisten verwenden Sie den Befehl `ipf.` Informationen zum Befehl `ipf` finden Sie in der Manpage `ipf(1M)`.

Sie erstellen die Paketfilterregeln entweder mithilfe des Befehls `ipf` in einer Befehlszeile oder in einer Paketfilterung-Konfigurationsdatei. Wenn Sie die Paketfilterregeln beim Booten laden möchten, erstellen Sie eine Konfigurationsdatei namens `/etc/ipf/ipf.conf` und legen die Regeln in dieser Datei an. Sollen die Paketfilterregeln nicht beim Booten geladen werden, speichern Sie die Datei `ipf.conf` in einen beliebigen Verzeichnis und aktivieren die Paketfilterung mithilfe des Befehls `ipf` manuell.

Mit Oracle Solaris IP Filter können Sie zwei Paketfilter-Regellisten verwalten: die aktive Regelliste und die inaktive Regelliste. In den meisten Fällen arbeiten Sie mit der aktiven Regelliste. Über den Befehl `ipf -I` können Sie die Befehlsaktion auch an der inaktiven Regelliste anwenden. Die inaktive Regelliste wird erst dann von Oracle Solaris IP Filter verwendet, wenn Sie sie auswählen. In der inaktiven Regelliste können Sie Regeln speichern, ohne dass sie sich auf die aktive Paketfilterung auswirken.

Oracle Solaris IP Filter arbeitet die Regeln in der Regelliste nacheinander vom dem Anfang der Liste bis zum Ende der Liste ab. Erst dann wird ein Paket durchgelassen oder blockiert. Oracle Solaris IP Filter setzt ein Flag, mit dem festgelegt wird, ob ein Paket durchgelassen wird oder nicht. Es durchläuft die gesamte Regelliste und legt fest, ob das Paket basierend auf der letzten übereinstimmenden Regel durchgelassen oder blockiert wird.

Für diesen Prozess gibt es zwei Ausnahmen. Die erste Ausnahme ist, wenn das Paket einer Regel entspricht, die das Schlüsselwort `quick` enthält. Wenn eine Regel das Schlüsselwort `quick` enthält, wird die Aktion für diese Regel ausgeführt und keine weiteren Regeln geprüft. Die

zweite Ausnahme ist, wenn ein Paket einer Regel entspricht, die das Schlüsselwort `group` enthält. Wenn ein Paket einer Gruppe entspricht, werden nur die Regeln geprüft, die dieser Gruppe zugeordnet sind.

Konfiguration der Paketfilterregeln

Zum Erstellen der Paketfilterregeln verwenden Sie die folgende Syntax:

Aktion `[in|out]` *Option Schlüsselwort, Schlüsselwort...*

1. Jede Regel beginnt mit einer Aktion. Oracle Solaris IP Filter wendet die Aktion an dem Paket an, wenn das Paket der Regel entspricht. Die folgende Liste enthält die Aktionen, die am häufigsten an einem Paket angewendet werden.

   `block` Verhindert, dass ein Paket den Filter passiert.

   `pass` Gestattet einem Paket, den Filter zu passieren.

   `log` Protokolliert das Paket, legt aber nicht fest, ob das Paket blockiert wird oder passieren darf. Zum Anzeigen des Protokolls verwenden Sie den Befehl `ipmon`.

   `Zählung` Nimmt das Paket in die Filterstatistiken auf. Zum Anzeigen der Statistiken verwenden Sie den Befehl `ipfstat`.

   `skip` *Zahl* Sorgt dafür, dass der Filter die nächsten *Zahl* Filterregeln überspringt.

   `auth` Fordert, dass die Paketauthentifizierung von einem Benutzerprogramm durchgeführt wird, dass die Paketinformationen überprüft. Das Programm legt fest, ob das Paket passieren darf oder blockiert wird.

   `preauth` Fordert, dass der Filter eine vorab authentifizierte Liste prüft, um festzustellen, was mit einem Paket erfolgen soll.

2. Nach dieser Aktion muss das nächste Wort entweder `in` oder `out` lauten. Ihre Auswahl legt fest, ob die Paketfilterregel an einem eingehenden Paket oder einem abgehenden Paket angewendet wird.

3. Als Nächstes können Sie in einer Optionsliste auswählen. Wenn Sie mehrere Optionen verwenden, müssen sie in der hier gezeigten Reihenfolge vorliegen.

   `log` Protokolliert das Paket, wenn die Regel die letzte übereinstimmende Regel ist. Zum Anzeigen des Protokolls verwenden Sie den Befehl `ipmon`.

   `quick` Führt die Regel aus, in der die Option `quick` enthalten ist, wenn eine Paketübereinstimmung aufgetreten ist. Anschließend werden keine weiteren Regeln geprüft.

   `on` *Schnittstellenname* Wendet die Regel nur dann an, wenn das Paket über die angegebene Schnittstelle ein- oder abgeht.

`dup-to` *Schnittstellenname*	Kopiert das Paket und sendet das Duplikat über *Schnittstellenname* an eine optional angegebene IP-Adresse.
`to` *Schnittstellenname*	Verschiebt das Paket über eine abgehende Warteschlange an *Schnittstellenname*.

4. Nach Angabe der Optionen können Sie unter zahlreichen Schlüsselwörtern wählen, mit denen festgestellt wird, ob das Paket der Regel entspricht. Die folgenden Schlüsselwörter müssen in der hier aufgeführten Reihenfolge verwendet werden.

Hinweis – Standardmäßig darf ein Paket, das keiner Regel in der Konfigurationsdatei entspricht, über den Filter passieren.

`tos`	Filtert das Paket basierend auf dem Servicetyp-Wert, der entweder als hexadezimale oder als dezimale ganze Zahl ausgedrückt ist.
`ttl`	Vergleicht die Pakete basierend auf dem Lebensdauerwert. Der in einem Paket gespeicherte Lebensdauerwert gibt an, wie lange sich ein Paket im Netzwerk aufhalten kann, bevor es gelöscht wird.
`proto`	Entspricht einem bestimmten Protokoll. Sie können einen der Protokollnamen in der Datei `/etc/protocols` oder eine Dezimalzahl verwenden, mit der das Protokoll angegeben wird. Mithilfe des Schlüsselworts `tcp/udp` kann z. B. geprüft werden, ob es sich um ein TCP- oder um ein UDP-Paket handelt.
`from/to/all/ any`	Vergleicht eine oder alle der folgenden Angaben: IP-Quelladresse, IP-Zieladresse und Portnummer. Mit dem Schlüsselwort `all` werden alle Pakete von allen Quellen und an alle Ziele akzeptiert.
`with`	Vergleicht bestimmte Attribute, die dem Paket zugeordnet sind. Fügen Sie entweder das Wort `not` oder das Wort `no` vor dem Schlüsselwort ein, damit ein Paket nur dann der Regel entspricht, wenn die Option nicht vorhanden ist.
`flags`	Wird bei TCP verwendet, um basierend auf gesetzten TCP-Flags zu filtern. Weitere Informationen zu den TCP-Flags finden Sie in der Manpage `ipf(4)`.
`icmp-type`	Filtert nach dem ICMP-Typ. Dieses Schlüsselwort wird nur dann verwendet, wenn die Option `proto` auf `icmp` gesetzt ist und nicht verwendet wird, wenn die Option `flags` aktiviert ist.
`keep` *keep-Optionen*	Legt die Informationen fest, die bei einem Paket beibehalten werden. Zu den verfügbaren *keep-Optionen* zählen die Optionen `state` und `frags.` Die Option `state` behält Informationen zur Sitzung bei und kann bei TCP-, UDP- und ICMP-Paketen

angewendet werden. Die Option `frags` behält Informationen zu Paketfragmenten bei und wendet diese Informationen an späteren Fragmenten an. Mit den *keep-Optionen* können entsprechende Pakete durchgelassen werden, ohne dass sie die Zugriffskontrolllisten durchlaufen müssen.

`head` *Zahl* — Erstellt eine neue Gruppe mit Filterregeln, die durch die Zahl *Zahl* gekennzeichnet ist.

`group` *Zahl* — Fügt die Regel zur Gruppennummer *Zahl* anstatt zur Standardgruppe hinzu. Wenn keine andere Gruppe angegeben wurde, werden alle Filterregeln werden in die Gruppe 0 eingefügt.

Das folgende Beispiel zeigt, wie die Syntax einer Paketfilterregel beim Erstellen einer Regel auszusehen hat. Zum Blockieren von eingehenden Verkehr von der IP-Adresse `192.168.0.0/16` nehmen Sie die folgende Regel in die Regelliste auf:

```
block in quick from 192.168.0.0/16 to any
```

Informationen zur vollständigen Grammatik und Syntax beim Schreiben von Paketfilterregeln finden Sie in der Manpage `ipf(4)` Aufgaben im Zusammenhang mit der Paketfilterung finden Sie unter „Verwalten der Paketfilter-Regellisten für Oracle Solaris IP Filter“ auf Seite 696. Eine Erklärung des im Beispiel verwendeten IP-Adressenschemas (`192.168.0.0/16`) finden Sie in Kapitel 2, „Planen Ihres TCP/IP-Netzwerks (Vorgehen)“.

Verwenden der NAT-Funktion in Oracle Solaris IP Filter

NAT stellt Zuordnungsregeln auf, die IP-Quell- und IP-Ziel-Adressen in andere Internet- oder Intranet-Adressen übersetzen. Diese Regeln ändern die Quell- und Zieladressen eingehender oder abgehender IP-Pakete und senden die Pakete weiter. Mit NAT können Sie Datenverkehr auch von einem Port an einen anderen Port umleiten. NAT behält die Integrität eines Datenpakets während Modifikationen oder Umleitungen des Pakets bei.

Zum Arbeiten mit NAT-Regellisten verwenden Sie den Befehl `ipnat.` Weitere Informationen zum Befehl `ipnat` finden Sie in der Manpage `ipnat(1M)`.

Sie erstellen die NAT-Regeln entweder mithilfe des Befehls `ipnat` in einer Befehlszeile oder in einer NAT-Konfigurationsdatei. NAT-Konfigurationsregeln werden in der Datei `ipnat.conf` angelegt. Wenn die NAT-Regeln beim Booten geladen werden soll, erstellen Sie eine Datei namens `/etc/ipf/ipnat.conf`, in der Sie die NAT-Regeln anlegen. Sollen die NAT-Regeln nicht beim Booten geladen werden, speichern Sie die Datei `ipnat.conf` in einem beliebigen anderen Verzeichnis und aktivieren die Paketfilterung mithilfe des Befehls `ipnat` manuell.

Konfiguration der NAT-Regeln

Zum Erstellen der NAT-Regeln verwenden Sie die folgende Syntax:

Befehl Schnittstellenname Parameter

1. Jede Regel beginnt mit einem der folgenden Befehle:

   `map` — Ordnet eine IP-Adresse oder ein Netzwerk einer anderen IP-Adresse oder einem Netzwerk zu. Dabei wird ein ungeregelter Round-Robin-Prozess verwendet.

   `rdr` — Leitet Pakete von einer IP-Adresse und einem Portpaar an eine andere IP-Adresse und ein anderes Portpaar um.

   `bimap` — Richtet eine bidirektionale NAT zwischen einer externen IP-Adresse und einer internen IP-Adresse ein.

   `map-block` — Richtet eine statische Übersetzung ein, die auf den IP-Adressen basiert. Dieser Befehl basiert auf einem Algorithmus, der die Übersetzung von Adressen in einen Zielbereich erzwingt.
2. Nach diesem Befehl muss das nächste Wort der Schnittstellenname sein, z. B. `hme0`.
3. Als Nächstes können Sie unter zahlreichen Parametern wählen, mit denen die NAT-Konfiguration festgelegt wird. Zu diesen Parametern zählen:

   `ipmask` — Entwirft die Netzwerkmaske.

   `dstipmask` — Weist die Adresse zu, in die `ipmask` übersetzt wird.

   `mapport` — Weist die Protokolle `tcp`, `udp` oder `tcp/udp` zusammen mit einem Portnummernbereich zu.

Das folgende Beispiel zeigt, wie mithilfe der Syntax für eine NAT-Regel eine NAT-Regel erstellt wird. Um ein Paket neu zu schreiben, das über das Gerät `de0` an die Zieladresse `192.168.1.0/24` gesendet wird, und um die Quelladresse extern als `10.1.0.0/16` anzuzeigen, nehmen Sie die folgende Regel in die NAT-Regelliste auf:

```
map de0 192.168.1.0/24 -> 10.1.0.0/16
```

Informationen zur vollständigen Grammatik und Syntax beim Schreiben von NAT-Regeln finden Sie in der Manpage `ipnat(4)`.

Verwenden der Adresspool-Funktion in Oracle Solaris IP Filter

Adresspools stellen eine Referenz dar, die zum Benennen einer Gruppe von Adress/Netzmasken-Paaren verwendet wird. Adresspools bieten Prozesse, mit denen die Zeit

zum Finden von Entsprechungen zwischen IP-Adressen und Regeln verringert wird. Mit Adresspools lassen sich auch große Adressengruppen einfacher verwalten.

Die Konfigurationsregeln für Adresspools befinden sich in der Datei `ippool.conf.` Wenn die Adresspool-Regeln beim Booten geladen werden sollen, erstellen Sie eine Datei namens `/etc/ipf/ippool.conf`, in der Sie die Adresspool-Regeln anlegen. Sollen die Adresspool-Regeln nicht beim Booten geladen werden, speichern Sie die Datei `ippool.conf` in einem beliebigen anderen Verzeichnis und aktivieren die Paketfilterung mithilfe des Befehls `ippool` manuell.

Konfiguration von Adresspools

Zum Erstellen eines Adresspools verwenden Sie die folgende Syntax:

`table role =` *role-name* `type =` *storage-format* `number =` *reference-number*

`table` Definiert die Referenz für mehrere Adressen.

`role` Legt die Rolle des Pools in Oracle Solaris IP Filter fest. Derzeit ist `ipf` die einzige Rolle, auf die Sie verweisen können.

`type` Gibt das Speicherformat für den Pool an.

`number` Gibt die Referenznummer an, die von der Filterregel verwendet wird.

Um beispielsweise die Adressgruppe `10.1.1.1` und `10.1.1.2` und das Netzwerk `192.16.1.0` als Poolnummer `13` zu verweisen, nehmen Sie die folgende Regel in die Adresspool-Konfigurationsdatei auf:

```
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24 };
```

Um dann in einer Filterregel auf die Poolnummer `13` zu verweisen, erstellen Sie eine Regel ähnlich der Folgenden:

```
pass in from pool/13 to any
```

Beachten Sie, dass die Pooldatei vor der Regeldatei geladen werden muss, in der ein Verweis auf den Pool enthalten ist. Andernfalls ist der Pool, wie in der folgenden Ausgabe gezeigt, nicht definiert:

```
# ipfstat -io
empty list for ipfilter(out)
block in from pool/13(!) to any
```

Auch wenn Sie den Pools später hinzufügen, wird die Regelliste im Kernel nicht aktualisiert. Sie müssen die Regeldatei, in der auf den Pool verwiesen wird, neu laden.

Informationen zur vollständigen Grammatik und Syntax beim Schreiben von Paketfilterregeln finden Sie in der Manpage ippool(4).

Paket Filter-Hooks

Ab Version Solaris 10 7/07 ersetzen die Paketfilter-Hooks das Modul pfil, um Oracle Solaris IP Filter zu aktivieren. In früheren Oracle Solaris-Versionen musste das Modul pfil in einem zusätzlichen Schritt beim Einrichten von Oracle Solaris IP Filter konfiguriert werden. Dieser zusätzliche Konfigurationsaufwand erhöhte das Risiko, das Oracle Solaris IP Filter fehlerhaft arbeitet. Durch Einfügen des pfil STREAMS-Moduls zwischen IP und dem Gerätetreiber wurde darüber hinaus eine Leistungsverschlechterung verursacht. Darüber hinaus konnte das pfil-Modul keine Pakete zwischen Zonen abfangen.

Mit der Verwendung der Paketfilter-Hooks wird das Verfahren zum Aktivieren von Oracle Solaris IP Filter rationalisiert. Aufgrund dieser Hooks verwendet Oracle Solaris IP Filter Prä-Routing- (Eingang) und Post-Routing-Filterabgriffe (Ausgang), um den ein- und abgehenden Paketfluss von Oracle Solaris-Systemen zu steuern.

Mit Paketfilter-Hooks ist das Modul pfil überflüssig geworden. Aus diesem Grund wurden auch die folgenden Komponenten entfernt, die zum Modul gehörten.

- pfil-Treiber
- pfil-Daemon
- svc:/network/pfil SMF-Service

Aufgaben im Zusammenhang mit der Aktivierung von Oracle Solaris IP Filter finden Sie in Kapitel 26, „Oracle Solaris IP Filter (Aufgaben)“.

Oracle Solaris IP Filter und das pfil STREAMS-Modul

Hinweis – Das Modul pfil wird nur in den folgenden Oracle Solaris 10-Versionen mit Oracle Solaris IP Filter verwendet:

- Solaris 10 3/05
- Solaris 10 1/06
- Solaris 10 6/06
- Solaris 10 11/06

Mit der Version Solaris 10 7/07 wurde das pfil-Modul durch die Paketfilter-Hooks ersetzt und wird nicht mehr mit Oracle Solaris IP Filter verwendet.

Das pfil STREAMS-Modul ist für die Arbeit mit Oracle Solaris IP Filter erforderlich. Oracle Solaris IP Filter bietet jedoch keinen automatischen Mechanismus, um das Modul auf jeder Schnittstelle bereitzustellen. Stattdessen wird das pfil STREAMS-Modul vom SMF-Service svc:/network/pfil verwaltet. Um die Filterung auf einer Netzwerkschnittstelle zu aktivieren, müssen Sie zunächst die Datei pfil.ap konfigurieren. Dann aktivieren Sie den svc:/network/pfil-Service, um der Netzwerkschnittstelle das pfil STREAMS-Modul bereitzustellen. Damit das STREAMS-Modul wirksam wird, muss das System entweder neu gebootet werden oder jede Netzwerkschnittstelle, für die eine Filterung angewendet werden soll, muss zunächst abgemeldet und dann erneut geplumbt (aktiviert) werden. Zum Aktivieren der IPv6-Paketfilterung müssen Sie die inet6-Version der Schnittstelle plumben anmelden.

Falls keine pfil-Module für Netzwerkschnittstellen gefunden wurden, werden die SMF-Services in den Wartungszustand versetzt. Die häufigste Ursache hierfür ist eine falsch bearbeitete Datei /etc/ipf/pfil.ap. Wenn der Service in den Wartungsmodus versetzt wird, wird dies in den Protokolldateien der Filterung aufgezeichnet.

Aufgaben im Zusammenhang mit der Aktivierung von Oracle Solaris IP Filter finden Sie unter „Konfiguration von Oracle Solaris IP Filter“ auf Seite 681.

IPv6 für Oracle Solaris IP Filter

Ab dem Solaris-Version 10 6/06 ist eine Unterstützung für IPv6 mit Oracle Solaris IP Filter verfügbar. Die IPv6-Paketfilterung kann basierend auf der Quell- oder Ziel-IPv6-Adresse, auf IPv6-Adresspools sowie auf IPv6-Extension-Header erfolgen.

IPv6 ähnelt IPv4 in vielerlei Hinsicht. Jedoch unterscheiden sich die Header- und Paketgrößen zwischen den zwei IP-Versionen; ein wichtiger Aspekt für IP Filter. IPv6-Pakete werden auch als *Jumbogramme* bezeichnet und enthalten ein Datagramm mit einer Länge von mehr als 65.535 Byte. Oracle Solaris IP Filter unterstützt keine IPv6-Jumbogramme. Informationen zu weiteren IPv6-Funktionen finden Sie unter „Die wichtigsten Leistungsmerkmale von IPv6“ auf Seite 74.

Hinweis – Weitere Informationen zu Jumbogrammen finden Sie in dem Dokument „IPv6 Jumbograms“, RFC 2675 von der Internet Engineering Task Force (IETF). [http://www.ietf.org/rfc/rfc2675.txt]

Die IP Filter-Aufgaben bei IPv6 unterscheiden sich nur wenig von denen bei IPv4. Der wichtigste Unterschied ist das Verwenden der Option -6 bei bestimmten Befehlen. Beispielsweise enthalten die Befehle ipf und ipfstat die Option -6, wenn sie mit der IPv6-Paketfilterung verwendet werden. Sie verwenden die Option -6 mit dem Befehl ipf zum Laden und Leeren der IPv6-Paketfilterregeln. Zum Anzeigen der IPv6-Statistiken verwenden Sie die Option -6 mit dem Befehl ipfstat. Auch die Befehle ipmon und ippool unterstützen

IPv6, obwohl es keine zugeordnete Funktion zur Unterstützung von IPv6 gibt. Der Befehl `ipmon` wurde erweitert, um die Protokollierung von IPv6-Paketen zu ermöglichen. Der Befehl `ippool` unterstützt IPv6-Adresspools. Sie können Pools erstellen, die entweder ausschließlich IPv4- oder IPv6-Adressen enthalten, oder einen Pool, der sowohl IPv4- als auch IPv6-Adressen enthält.

Mit der Datei `ipf6.conf` erstellen Sie Paketfilter-Regellisten für IPv6. Standardmäßig befindet sich die Konfigurationsdatei `ipf6.conf` in dem Verzeichnis `/etc/ipf.` Wie andere Konfigurationsdateien zur Paketfilterung wird die Datei `ipf6.conf` automatisch während des Bootens geladen, wenn sie sich im Verzeichnis `/etc/ipf` befindet. Sie können eine IPv6-Konfigurationsdatei auch in einem beliebigen anderen Verzeichnis speichern und dann manuell laden.

Hinweis – Network Address Translation (NAT) unterstützt IPv6 nicht.

Nachdem Paketfilterregeln für IPv6 aufgestellt wurden, aktivieren Sie die IPv6-Paketfilterung, indem Sie die `inet6`-Version der Schnittstelle plumben (aktivieren).

Weitere Informationen zu IPv6 finden Sie in Kapitel 3, „Einführung in IPv6 (Überblick)“. Aufgaben im Zusammenhang mit der Aktivierung von Oracle Solaris IP Filter finden Sie in Kapitel 26, „Oracle Solaris IP Filter (Aufgaben)“.

Oracle Solaris IP Filter – Manpages

Die folgende Tabelle enthält eine Liste der Manpage-Dokumentation für Oracle Solaris IP Filter.

Manpage	Beschreibung
`ipf(1M)`	Verwenden des Befehls `ipf`, um die folgenden Aufgaben abzuschließen: ■ Arbeiten mit Paketfilter-Regellisten. ■ Aktivieren und Deaktivieren der Filterung. ■ Zurücksetzen von Statistiken und Neusynchronisieren der Kernel-internen Schnittstellenliste mit der aktuellen Schnittstellen-Statusliste.
`ipf(4)`	Enthält die Grammatik und Syntax zum Erstellen von Oracle Solaris IP Filter-Paketfilterregeln.
`ipfilter(5)`	Enthält Lizenzinformationen zum Open Source IP Filter.

Manpage	Beschreibung
ipfs(1M)	Verwenden des Befehls ipfs zum Speichern und Wiederherstellen der NAT-Informationen und Statustabelleninformationen nach Neustarts.
ipfstat(1M)	Verwenden des Befehls ipfstat zum Abrufen und Anzeigen von Statistiken zur Paketverarbeitung.
ipmon(1M)	Verwenden des Befehls ipmon zum Öffnen des Protokollierungsgeräts und zum Anzeigen der protokollierten Pakete für Paketfilterung und NAT.
ipnat(1M)	Verwenden des Befehls ipnat zum Abschließen der folgenden Aufgaben: ■ Arbeiten mit NAT-Regeln. ■ Abrufen und Anzeigen von NAT-Statistiken.
ipnat(4)	Enthält die Grammatik und Syntax zum Erstellen von NAT-Regeln.
ippool(1M)	Verwenden des Befehls ippool zum Erstellen und Verwalten von Adresspools.
ippool(4)	Enthält die Grammatik und Syntax zum Erstellen von Oracle Solaris IP Filter-Adresspools.
ndd(1M)	Anzeige der aktuellen Filterparameter des pfil STREAMS-Moduls und der aktuellen Werte der einstellbaren Parameter.

KAPITEL 26

Oracle Solaris IP Filter (Aufgaben)

In diesem Kapitel finden Sie schrittweise Anweisungen zum Arbeiten mit Solaris IP Filter. Eine Einführung in Oracle Solaris IP Filter finden Sie in Kapitel 25, „Oracle Solaris IP Filter (Übersicht)“.

Dieses Kapitel enthält die folgenden Informationen:

- „Konfiguration von Oracle Solaris IP Filter“ auf Seite 681
- „Deaktivieren und Stoppen von Oracle Solaris IP Filter“ auf Seite 685
- „Arbeiten mit dem `pfil`-Modul“ auf Seite 688
- „Arbeiten mit Oracle Solaris IP Filter-Regellisten“ auf Seite 695
- „Anzeigen von Statistiken und Informationen zu Oracle Solaris IP Filter“ auf Seite 707
- „Arbeiten mit Protokolldateien für Oracle Solaris IP Filter“ auf Seite 710
- „Erstellen und Bearbeiten von Konfigurationsdateien für Oracle Solaris IP Filter“ auf Seite 714

Konfiguration von Oracle Solaris IP Filter

In der folgenden Tabelle sind die Verfahren zur Konfiguration von Oracle Solaris IP Filter aufgeführt.

TABELLE 26–1 Konfiguration von Oracle Solaris IP Filter (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Erstaktivierung von Oracle Solaris IP Filter.	Oracle Solaris IP Filter ist standardmäßig nicht aktiviert. Sie müssen Solaris IP Filter entweder manuell aktivieren oder die Konfigurationsdateien im Verzeichnis `/etc/ipf/` verwenden und das System neu booten. Ab Version Solaris 10 7/07 ersetzen die Paketfilter-Hooks das Modul `pfil`, um Oracle Solaris IP Filter zu aktivieren.	„So aktivieren Sie Oracle Solaris IP Filter" auf Seite 682
Erneutes Aktivieren von Oracle Solaris IP Filter.	Falls Oracle Solaris IP Filter deaktiviert oder abgeschaltet wurde, können Sie Oracle Solaris IP Filter neu aktivieren, indem Sie entweder das System neu booten oder den Befehl `ipf` eingeben.	„So aktivieren Sie Oracle Solaris IP Filter erneut" auf Seite 683
Aktivieren der Loopback-Filterung	Optional können Sie die Loopback-Filterung aktivieren, um beispielsweise Datenverkehr zwischen Zonen zu filtern.	„So aktivieren Sie die Loopback-Filterung" auf Seite 684

▼ So aktivieren Sie Oracle Solaris IP Filter

Mit dem folgenden Verfahren aktivieren Sie Oracle Solaris IP Filter auf einem System, das mindestens Solaris 10 7/07 ausführt. Um Oracle Solaris IP Filter auch dann auszuführen, wenn ein Solaris Oracle Solaris 10-Version vor Solaris 10 7/07 ausgeführt wird, lesen Sie „Arbeiten mit dem `pfil`-Modul" auf Seite 688.

1 Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.

Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Erstellen Sie eine Paketfilter-Regelliste.

Die Paketfilter-Regelliste enthält Regeln, die von Oracle Solaris IP Filter verwendet werden. Wenn die Paketfilterregeln beim Booten geladen werden sollen, müssen Sie die Datei `/etc/ipf/ipf.conf` so bearbeiten, dass sie die IPv4-Paketfilterung implementiert. Für IPv6-Paketfilterregeln verwenden Sie die Datei `/etc/ipf/ipf6.conf`. Sollen die Paketfilterregeln nicht beim Booten geladen werden, speichern Sie die Regeln in einer Datei in

einem beliebigen Verzeichnis und aktivieren die Paketfilterung dann manuell. Informationen zur Paketfilterung finden Sie unter „Verwenden der Paketfilter-Funktionen in Oracle Solaris IP Filter“ auf Seite 671. Informationen zum Arbeiten mit Konfigurationsdateien finden Sie unter „Erstellen und Bearbeiten von Konfigurationsdateien für Oracle Solaris IP Filter“ auf Seite 714.

3. **(Optional) Erstellen Sie eine Network Address Translation (NAT)-Konfigurationsdatei.**

Hinweis – Network Address Translation (NAT) unterstützt IPv6 nicht.

Erstellen Sie eine Datei `ipnat.conf`, wenn Sie die Network Address Translation verwenden möchten. Wenn die NAT-Regeln beim Booten geladen werden soll, erstellen Sie eine Datei namens `/etc/ipf/ipnat.conf`, in der Sie die NAT-Regeln anlegen. Sollen die NAT-Regeln nicht beim Booten geladen werden, speichern Sie die Datei `ipnat.conf` in einem beliebigen anderen Verzeichnis und aktivieren die NAT-Regeln dann manuell.

Weitere Informationen zu NAT finden Sie unter „Verwenden der NAT-Funktion in Oracle Solaris IP Filter“ auf Seite 674.

4. **(Optional) Erstellen Sie eine Adresspool-Konfigurationsdatei.**

Erstellen Sie eine Datei `ipool.conf`, wenn Sie eine Adressengruppe als einen Adresspool ansprechen möchten. Wenn die Adresspool-Konfigurationsdatei beim Booten geladen werden soll, erstellen Sie eine Datei namens `/etc/ipf/ippool.conf`, in der Sie den Adresspool anlegen. Soll die Adresspool-Konfiguration nicht beim Booten geladen werden, speichern Sie die Datei `ippool.conf` in einem beliebigen anderen Verzeichnis und aktivieren die Regeln dann manuell.

Ein Adresspool kann entweder nur IPv4-Adressen oder nur IPv6-Adressen enthalten. Er kann auch sowohl IPv4- als auch IPv6-Adressen enthalten.

Weitere Informationen zu Adresspools finden Sie unter „Verwenden der Adresspool-Funktion in Oracle Solaris IP Filter“ auf Seite 675.

5. **(Optional) Aktivieren Sie die Filterung von Loopback-Verkehr.**

Falls Sie beabsichtigen, Datenverkehr zwischen auf Ihrem System konfigurierten Zonen zu filtern, müssen Sie die Loopback-Filterung aktivieren. Lesen Sie dazu „So aktivieren Sie die Loopback-Filterung“ auf Seite 684. Denken in Sie daran, entsprechende Regellisten für die Zonen zu definieren.

6. **Aktivieren Sie Oracle Solaris IP Filter.**

```
# svcadm enable network/ipfilter
```

▼ So aktivieren Sie Oracle Solaris IP Filter erneut

Sie können die Paketfilterung neu aktivieren, nachdem sie vorübergehend deaktiviert wurde.

1 Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.

Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services* .

2 Starten Sie Oracle Solaris IP Filter und aktivieren Sie die Filterung mithilfe einer der folgenden Methoden:

- Starten Sie den Computer neu.

  ```
  # reboot
  ```

  Hinweis – Wenn IP Filter aktiviert ist, werden bei einem Neustart die folgenden Dateien geladen, sofern sie vorhanden sind: die Datei `/etc/ipf/ipf.conf`, die Datei `/etc/ipf/ipf6.conf`, wenn IPv6 verwendet wird , oder die Datei `/etc/ipf/ipnat.conf`.

- Rufen Sie die folgenden Befehle auf, um Oracle Solaris IP Filter zu starten und die Filterung zu aktivieren:

  a. Aktivieren Sie Oracle Solaris IP Filter.

  ```
  # ipf -E
  ```

  b. Aktivieren Sie die Paketfilterung.

  ```
  # ipf -f filename
  ```

  c. (Optional) Aktivieren Sie NAT.

  ```
  # ipnat -f filename
  ```

  Hinweis – Network Address Translation (NAT) unterstützt IPv6 nicht.

▼ So aktivieren Sie die Loopback-Filterung

Hinweis – Sie können Loopback-Verkehr nur dann filtern, wenn Ihr System mindestens Version Solaris 10 7/07 ausführt. In älteren Oracle Solaris 10-Versionen wird die Loopback-Filterung nicht unterstützt.

---

1 Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.

Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services* .

2 Halten Sie Oracle Solaris IP Filter an, wenn es ausgeführt wird.

```
# svcadm disable network/ipfilter
```

3 Fügen Sie die folgende Zeile am Anfang der Datei `/etc/ipf.conf` **bzw. der Datei** `/etc/ipf6.conf` **ein:**

```
set intercept_loopback true;
```

Die Zeile muss vor allen IP-Filterregeln stehen, die in der Datei definiert sind. Sie können Befehle auch vor dieser Zeile einfügen. Betrachten Sie dazu das folgende Beispiel:

```
#
# Enable loopback filtering to filter between zones
#
set intercept_loopback true;
#
# Define policy
#
block in all
block out all
<other rules>
...
```

4 Starten Sie Oracle Solaris IP Filter.

```
# svcadm enable network/ipfilter
```

5 Geben Sie den folgenden Befehl ein, um den Status der Loopback-Filterung zu überprüfen:

```
# ipf –T ipf_loopback
ipf_loopback    min 0   max 0x1 current 1
#
```

Wenn die Loopback-Filterung deaktiviert ist, erzeugt der Befehl die folgende Ausgabe:

```
ipf_loopback    min 0   max 0x1 current 0
```

Deaktivieren und Stoppen von Oracle Solaris IP Filter

Eventuell muss die Paketfilterung und NAT unter den folgenden Umständen deaktiviert und gestoppt werden:

- Zu Testzwecken
- Zur Fehlerbehandlung von Systemproblemen, wenn Sie glauben, die Probleme werden durch Oracle Solaris IP Filter verursacht

In der folgenden Tabelle sind die Verfahren zum Deaktivieren bzw. zum Stoppen der Oracle Solaris IP Filter-Funktionen aufgeführt.

TABELLE 26–2 Deaktivieren und stoppen von Oracle Solaris IP Filter (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Deaktivieren der Paketfilterung.	Deaktivieren Sie die Paketfilterung mithilfe des Befehls `ipf`.	„So deaktivieren Sie die Paketfilterung“ auf Seite 686
Deaktivieren der NAT.	Deaktivieren Sie die NAT mithilfe des Befehls `ipnat`.	„So deaktivieren Sie NAT“ auf Seite 687
Stoppen von Paketfilterung und NAT.	Stoppen Sie die Paketfilterung und NAT mithilfe des Befehls `ipf`.	„So stoppen Sie die Paketfilterung“ auf Seite 687

▼ So deaktivieren Sie die Paketfilterung

Mit dem folgenden Verfahren deaktivieren Sie die Oracle Solaris IP Filter-Paketfilterung, indem Sie die Paketfilterregeln aus der aktiven Regelliste entfernen. Mit diesem Verfahren wird Oracle Solaris IP Filter nicht gestoppt. Sie können Oracle Solaris IP Filter neu aktivieren, indem Sie Regeln wieder zur Regelliste hinzufügen.

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

2. **Führen Sie eine Methoden aus, um die Oracle Solaris IP Filter-Regeln zu deaktivieren:**

   - Entfernen Sie die aktive Regelliste aus dem Kernel.

     ```
     # ipf -Fa
     ```

     Dieser Befehl deaktiviert die Paketfilterregeln.

   - Entfernen Sie die Filterregeln für eingehende Pakete.

     ```
     # ipf -Fi
     ```

     Dieser Befehl deaktiviert die Paketfilterregeln für eingehende Pakete.

   - Entfernen Sie die Filterregeln für abgehende Pakete.

     ```
     # ipf -Fo
     ```

     Dieser Befehl deaktiviert die Paketfilterregeln für abgehende Pakete.

So deaktivieren Sie NAT

Mit dem folgenden Verfahren deaktivieren Sie die Oracle Solaris IP Filter-NAT-Regeln, indem Sie die NAT-Regeln aus der aktiven NAT-Regelliste entfernen. Mit diesem Verfahren wird Oracle Solaris IP Filter nicht deaktiviert. Sie können Oracle Solaris IP Filter neu aktivieren, indem Sie Regeln wieder zur Regelliste hinzufügen.

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Entfernen Sie die NAT aus dem Kernel.**

   ```
   # ipnat -FC
   ```

   Die Option `-C` löscht alle Einträge aus der aktuellen NAT-Regelliste. Mit der Option `-F` entfernen Sie alle aktiven Einträge aus der aktuellen NAT-Übersetzungstabelle, in der die derzeit aktiven NAT-Zuordnungen aufgeführt sind.

So stoppen Sie die Paketfilterung

Wenn Sie dieses Verfahren ausführen, werden sowohl Paketfilterung als auch NAT aus dem Kernel entfernt. Nachdem Sie dieses Verfahren ausgeführt haben, müssen Sie Solaris IP Filter neu starten, um die Paketfilterung und NAT zu reaktivieren. Weitere Informationen finden Sie unter „So aktivieren Sie Oracle Solaris IP Filter erneut“ auf Seite 683.

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Stoppen Sie die Paketfilterung und gestatten Sie, dass alle Pakete in das Netzwerk passieren.**

   ```
   # ipf –D
   ```

Hinweis – Mit dem Befehl `ipf -D` entfernen Sie die Regeln aus der Regelliste. Wenn Sie die Filterung neu starten möchten, müssen Sie die Regeln wieder zur Regelliste hinzufügen.

Arbeiten mit dem pfil-Modul

In diesem Abschnitt wird beschrieben, wie Sie das pfil STREAMS-Modul zum Aktivieren oder Deaktivieren von Oracle Solaris IP Filter verwenden und pfil-Statistiken anzeigen. Diese Verfahren gelten nur für Systeme, die eines der folgenden Oracle Solaris-Versionen ausführen:

- Solaris 10 3/05
- Solaris 10 1/06
- Solaris 10 6/06
- Solaris 10 11/06

In der folgenden Tabelle sind die Verfahren aufgeführt, mit denen das pfil-Modul konfiguriert wird.

TABELLE 26–3 Arbeiten mit dem pfil-Modul (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Aktivieren von Oracle Solaris IP Filter	Oracle Solaris IP Filter ist standardmäßig nicht aktiviert. Sie müssen Solaris IP Filter entweder manuell aktivieren oder die Konfigurationsdateien im Verzeichnis /etc/ipf/ verwenden und das System neu booten.	„So aktivieren Sie Oracle Solaris IP Filter in älteren Solaris Oracle Solaris-Versionen“ auf Seite 688
Aktivieren einer NIC zur Paketfilterung	Konfigurieren Sie das pfil-Modul, um die Paketfilterung auf einer NIC zu aktivieren	„So aktivieren Sie eine NIC für die Paketfilterung“ auf Seite 691
Deaktivieren von Oracle Solaris IP Filter auf einer NIC	Entfernen Sie eine NIC und gestatten Sie, dass alle Pakete eine NIC passieren.	„So deaktivieren Sie Oracle Solaris IP Filter auf einer NIC“ auf Seite 692
Anzeigen der pfil-Statistiken.	Die Statistiken des pfil-Moduls helfen Ihnen bei der Fehlerbehebung von Oracle Solaris IP Filter mit dem Befehl ndd.	„So zeigen Sie die pfil-Statistiken für Oracle Solaris IP Filter an“ auf Seite 694

▼ So aktivieren Sie Oracle Solaris IP Filter in älteren Solaris Oracle Solaris-Versionen

Oracle Solaris IP Filter wird mit Oracle Solaris installiert;. Die Paketfilterung wird jedoch standardmäßig nicht aktiviert. Verwenden Sie das folgende Verfahren, um Oracle Solaris IP Filter zu aktivieren.

Hinweis – Falls auf Ihrem System mindestens Solaris 10 7/07 ausgeführt wird, befolgen Sie das Verfahren„So aktivieren Sie Oracle Solaris IP Filter" auf Seite 682, bei dem Eingriffspunkte für Paketfilter eingesetzt werden.

---

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2. **Starten Sie einen Dateieditor und nehmen Sie Änderungen an der Datei** `/etc/ipf/pfil.ap` **vor.**

   Diese Datei enthält die Namen der Netzwerkschnittstellenkarten (NICs) auf dem Host. Standardmäßig sind diese Namen auskommentiert. Löschen Sie das Kommentarzeichen für Geräte, die den zu filternden Netzwerkverkehr übertragen. Sollte der Name der NIC für Ihr System nicht aufgeführt sein, fügen Sie eine Zeile hinzu, in der diese NIC angegeben wird.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor lastminor modules

#le     -1      0       pfil
#qe     -1      0       pfil
hme     -1      0       pfil (Device has been uncommented for filtering)
#qfe    -1      0       pfil
#eri    -1      0       pfil
#ce     -1      0       pfil
#bge    -1      0       pfil
#be     -1      0       pfil
#vge    -1      0       pfil
#ge     -1      0       pfil
#nf     -1      0       pfil
#fa     -1      0       pfil
#ci     -1      0       pfil
#el     -1      0       pfil
#ipdptp -1      0       pfil
#lane   -1      0       pfil
#dmfe   -1      0       pfil
```

3. **Aktivieren Sie Ihre Änderungen an der Datei** `/etc/ipf/pfil.ap`**, indem Sie die Serviceinstanz** `network/pfil` **neu starten.**

```
# svcadm restart network/pfil
```

4. **Erstellen Sie eine Paketfilter-Regelliste.**

   Die Paketfilter-Regelliste enthält Regeln, die von Oracle Solaris IP Filter verwendet werden. Wenn die Paketfilterregeln beim Booten geladen werden sollen, müssen Sie die Datei

/etc/ipf/ipf.conf so bearbeiten, dass sie die IPv4-Paketfilterung implementiert. Für IPv6-Paketfilterregeln verwenden Sie die Datei /etc/ipf/ipf6.conf. Sollen die Paketfilterregeln nicht beim Booten geladen werden, speichern Sie die Regeln in einer Datei in einem beliebigen Verzeichnis und aktivieren die Paketfilterung dann manuell. Informationen zur Paketfilterung finden Sie unter „Verwenden der Paketfilter-Funktionen in Oracle Solaris IP Filter“ auf Seite 671. Informationen zum Arbeiten mit Konfigurationsdateien finden Sie unter „Erstellen und Bearbeiten von Konfigurationsdateien für Oracle Solaris IP Filter“ auf Seite 714.

5 (Optional) Erstellen Sie eine Network Address Translation (NAT)-Konfigurationsdatei.

Hinweis – Network Address Translation (NAT) unterstützt IPv6 nicht.

Erstellen Sie eine Datei ipnat.conf, wenn Sie die Network Address Translation verwenden möchten. Wenn die NAT-Regeln beim Booten geladen werden soll, erstellen Sie eine Datei namens /etc/ipf/ipnat.conf, in der Sie die NAT-Regeln anlegen. Sollen die NAT-Regeln nicht beim Booten geladen werden, speichern Sie die Datei ipnat.conf in einem beliebigen anderen Verzeichnis und aktivieren die NAT-Regeln dann manuell.

Weitere Informationen zu NAT finden Sie unter „Verwenden der NAT-Funktion in Oracle Solaris IP Filter“ auf Seite 674.

6 (Optional) Erstellen Sie eine Adresspool-Konfigurationsdatei.

Erstellen Sie eine Datei ipool.conf, wenn Sie eine Adressengruppe als einen Adresspool ansprechen möchten. Wenn die Adresspool-Konfigurationsdatei beim Booten geladen werden soll, erstellen Sie eine Datei namens /etc/ipf/ippool.conf, in der Sie den Adresspool anlegen. Soll die Adresspool-Konfiguration nicht beim Booten geladen werden, speichern Sie die Datei ippool.conf in einem beliebigen anderen Verzeichnis und aktivieren die Regeln dann manuell.

Ein Adresspool kann entweder nur IPv4-Adressen oder nur IPv6-Adressen enthalten. Er kann auch sowohl IPv4- als auch IPv6-Adressen enthalten.

Weitere Informationen zu Adresspools finden Sie unter „Verwenden der Adresspool-Funktion in Oracle Solaris IP Filter“ auf Seite 675.

7 Aktivieren Sie Oracle Solaris IP Filter mithilfe einer der folgenden Methoden:

- Aktivieren Sie IP Filter und starten Sie den Computer neu.

```
# svcadm enable network/ipfilter
# reboot
```

Hinweis – Ein Neustart ist erforderlich, wenn Sie die Befehle ifconfig unplumb und ifconfig plumb nicht sicher auf den NICs verwenden können.

- Aktivieren Sie die NICs mithilfe der Befehle `ifconfig unplumb` und `ifconfig plumb`. Dann aktivieren Sie IP Filter. Die `inet6`-Version der Schnittstelle muss geplumbt (aktiviert) werden, um eine IPv6-Paketfilterung zu implementieren.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20 netmask 255.255.255.0 up
# ifconfig hme0 inte6 unplumb
# ifconfig hme0 inet6 plumb fec3:f849::1/96 up
# svcadm enable network/ipfilter
```

Weitere Informationen zum Befehl `ifconfig` finden Sie in der Manpage `ifconfig`(1M).

So aktivieren Sie eine NIC für die Paketfilterung

Oracle Solaris IP Filter wird beim Booten aktiviert, wenn die Datei `/etc/ipf/ipf.conf` (bzw. die Datei `/etc/ipf/ipf6.conf`, wenn IPv6 verwendet wird) vorhanden ist. Müssen Sie die Paketfilterung auf einer NIC aktivieren, nachdem Oracle Solaris IP Filter gestartet wurde, verwenden Sie das folgende Verfahren.

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Starten Sie einen Dateieditor und nehmen Sie Änderungen an der Datei `/etc/ipf/pfil.ap` vor.**

   Diese Datei enthält die Namen der NICs auf dem Host. Standardmäßig sind diese Namen auskommentiert. Löschen Sie das Kommentarzeichen für Geräte, die den zu filternden Netzwerkverkehr übertragen. Sollte der Name der NIC für Ihr System nicht aufgeführt sein, fügen Sie eine Zeile hinzu, in der diese NIC angegeben wird.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor lastminor modules

#le     -1      0       pfil
#qe     -1      0       pfil
hme     -1      0       pfil (Device has been uncommented for filtering)
#qfe    -1      0       pfil
#eri    -1      0       pfil
#ce     -1      0       pfil
#bge    -1      0       pfil
#be     -1      0       pfil
#vge    -1      0       pfil
#ge     -1      0       pfil
```

```
#nf     -1      0       pfil
#fa     -1      0       pfil
#ci     -1      0       pfil
#el     -1      0       pfil
#ipdptp -1      0       pfil
#lane   -1      0       pfil
#dmfe   -1      0       pfil
```

3 **Aktivieren Sie Ihre Änderungen an der Datei `/etc/ipf/pfil.ap`, indem Sie die Serviceinstanz `network/pfil` neu starten.**

```
# svcadm restart network/pfil
```

4 **Aktivieren Sie die NIC mithilfe einer der folgenden Methoden:**

- Starten Sie den Computer neu.

  ```
  # reboot
  ```

  Hinweis – Ein Neustart ist erforderlich, wenn Sie die Befehle `ifconfig unplumb` und `ifconfig plumb` nicht sicher auf den NICs verwenden können.

- Aktivieren Sie die NICs, wenn Sie die Filterung mithilfe des Befehls `ifconfig` und den Optionen `unplumb` und `plumb` vornehmen möchten. Die `inet6`-Version der Schnittstelle muss geplumbt (aktiviert) werden, um eine IPv6-Paketfilterung zu implementieren.

  ```
  # ifconfig hme0 unplumb
  # ifconfig hme0 plumb 192.168.1.20  netmask 255.255.255.0  up
  # ifconfig hme0 inet6 unplumb
  # ifconfig hme0 inet6 plumb fec3:f840::1/96 up
  ```

  Weitere Informationen zum Befehl `ifconfig` finden Sie in der Manpage `ifconfig`(1M).

▼ So deaktivieren Sie Oracle Solaris IP Filter auf einer NIC

Soll die Paketfilterung auf einer NIC gestoppt werden, verwenden Sie das folgende Verfahren.

1 **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2 Starten Sie einen Dateieditor und nehmen Sie Änderungen an der Datei `/etc/ipf/pfil.ap` vor.

Diese Datei enthält die Namen der NICs auf dem Host. Die NICs, die zur Filterung des Netzwerkverkehrs verwendet wurden, sind nicht mit einem Kommentarzeichen versehen. Versehen Sie die Geräte, deren Netzwerkverkehr nicht mehr gefiltert werden soll, mit einem Kommentarzeichen.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor lastminor modules

#le     -1      0       pfil
#qe     -1      0       pfil
#hme    -1      0       pfil (Commented-out device no longer filters network traffic)
#qfe    -1      0       pfil
#eri    -1      0       pfil
#ce     -1      0       pfil
#bge    -1      0       pfil
#be     -1      0       pfil
#vge    -1      0       pfil
#ge     -1      0       pfil
#nf     -1      0       pfil
#fa     -1      0       pfil
#ci     -1      0       pfil
#el     -1      0       pfil
#ipdptp -1      0       pfil
#lane   -1      0       pfil
#dmfe   -1      0       pfil
```

3 Deaktivieren Sie die NIC mithilfe einer der folgenden Methoden:

- Starten Sie den Computer neu.

  ```
  # reboot
  ```

  Hinweis – Ein Neustart ist erforderlich, wenn Sie die Befehle `ifconfig unplumb` und `ifconfig plumb` nicht sicher auf den NICs verwenden können.

- Deaktivieren Sie die NICs mithilfe des Befehls `ifconfig` und den Optionen `unplumb` und `plumb.` Für die `inet6`-Version jeder Schnittstelle muss das Plumbing aufgehoben (deaktiviert) werden, um die IPv6-Paketfilterung zu deaktivieren. Führen Sie die folgenden Schritte aus. Das Beispielgerät im System ist `hme`:

  a. Geben Sie die Hauptnummer des zu deaktivierenden Geräts an.

  ```
  # grep hme /etc/name_to_major
  hme 7
  ```

  b. Zeigen Sie die aktuelle `autopush`-Konfiguration für `hme0` an.

```
# autopush -g -M 7 -m 0
   Major     Minor     Lastminor       Modules
       7      ALL          -           pfil
```

c. Entfernen Sie die autopush-Konfiguration.

```
# autopush -r -M 7 -m 0
```

d. Öffnen Sie das Gerät und weisen Sie dem Gerät IP-Adressen zu.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20  netmask 255.255.255.0  up
# ifconfig hme0 inet6 unplumb
# ifconfig hme0 inet6 plumb fec3:f840::1/96 up
```

Weitere Informationen zum Befehl ifconfig finden Sie in der Manpage ifconfig(1M).

▼ So zeigen Sie die pfil-Statistiken für Oracle Solaris IP Filter an

Zur Fehlerbehebung bei Oracle Solaris IP Filter können Sie die pfil-Statistiken anzeigen.

1 Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.

Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2 Anzeigen der pfil-Statistiken.

```
# ndd -get /dev/pfil qif_status
```

Beispiel 26–1 Anzeigen der pfil-Statistiken für Oracle Solaris IP Filter

Im folgenden Beispiel wird gezeigt, wie Sie die **pfil**-Statistiken anzeigen.

```
# ndd -get /dev/pfil qif_status
ifname ill q OTHERQ num sap hl nr nw bad copy copyfail drop notip nodata
   notdata
QIF6 0 300011247b8 300011248b0 6 806 0 4 9 0 0 0 0 0 0 0
dmfe1 3000200a018 30002162a50 30002162b48 5 800 14 171 13681 0 0 0 0 0 0 0
```

Arbeiten mit Oracle Solaris IP Filter-Regellisten

In der folgenden Tabelle sind die Verfahren zum Arbeiten mit den Oracle Solaris IP Filter-Regellisten aufgeführt.

TABELLE 26–4 Arbeiten mit den Oracle Solaris IP Filter-Regellisten (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Verwalten, Anzeigen und Ändern von Regellisten zur Oracle Solaris IP Filter-Paketfilterung.		„Verwalten der Paketfilter-Regellisten für Oracle Solaris IP Filter" auf Seite 696
	Zeigen Sie eine aktive Paketfilter-Regelliste an.	„So zeigen Sie die aktive Paketfilter-Regelliste an" auf Seite 696
	Zeigen Sie eine inaktive Paketfilter-Regelliste an.	„So zeigen Sie die inaktive Paketfilter-Regelliste an" auf Seite 697
	Aktivieren Sie eine andere aktive Regelliste.	„So aktivieren Sie eine andere oder aktualisierte Paketfilter-Regelliste" auf Seite 697
	Entfernen Sie eine Regelliste.	„So entfernen Sie eine Paketfilter-Regelliste" auf Seite 699
	Fügen Sie zusätzliche Regeln zu Regellisten hinzu.	„So fügen Sie der aktiven Paketfilter-Regelliste Regeln hinzu" auf Seite 699
		„So fügen Sie der inaktiven Paketfilter-Regelliste Regeln hinzu" auf Seite 700
	Wechseln Sie zwischen aktiven und inaktiven Regellisten.	„So wechseln Sie zwischen der aktiven und der inaktiven Paketfilter-Regelliste" auf Seite 701
	Löschen Sie eine inaktive Regelliste aus dem Kernel.	„So entfernen Sie eine inaktive Paketfilter-Regelliste aus dem Kernel" auf Seite 702
Verwalten, Anzeigen und Ändern von Oracle Solaris IP Filter-NAT-Regeln.		„Verwalten der NAT-Regeln für Oracle Solaris IP Filter" auf Seite 703
	Zeigen Sie aktive NAT-Regeln an.	„So zeigen Sie die aktiven NAT-Regeln an" auf Seite 703

TABELLE 26–4 Arbeiten mit den Oracle Solaris IP Filter-Regellisten (Übersicht der Schritte) *(Fortsetzung)*

Aufgabe	Beschreibung	Siehe
	Entfernen Sie NAT-Regeln.	„So entfernen Sie NAT-Regeln“ auf Seite 703
	Fügen Sie zusätzliche Regeln zu NAT-Regeln hinzu.	„So hängen Sie Regeln an die NAT-Regelliste an“ auf Seite 704
Verwalten, Anzeigen und Ändern von Oracle Solaris IP Filter-Adresspools.		„Verwalten der Adresspools für Oracle Solaris IP Filter“ auf Seite 705
	Zeigen Sie aktive Adresspools an.	„So zeigen Sie die aktiven Adresspools an“ auf Seite 705
	Entfernen Sie einen Adresspool.	„So entfernen Sie einen Adresspool“ auf Seite 705
	Fügen Sie zusätzliche Regeln zu einem Adresspool hinzu.	„So hängen Sie Regeln an einen Adresspool an“ auf Seite 706

Verwalten der Paketfilter-Regellisten für Oracle Solaris IP Filter

Wenn Solaris IP Filter aktiviert ist, können sowohl aktive als auch inaktive Paketfilter-Regellisten im Kernel gespeichert sein. Die aktive Regelliste legt fest, welche Filterung an eingehenden und abgehenden Paketen durchgeführt wird. Auch in der inaktiven Regelliste sind Regeln gespeichert. Diese Regeln werden jedoch nicht verwendet, bis Sie die inaktive Regelliste zur aktiven Regelliste machen. Sie können sowohl die aktive als auch die inaktive Paketfilter-Regelliste verwalten, anzeigen und ändern.

▼ So zeigen Sie die aktive Paketfilter-Regelliste an

1 Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.

Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2 Zeigen Sie die aktive Paketfilter-Regelliste an, die in den Kernel geladen wurde.

```
# ipfstat -io
```

Beispiel 26–2 Anzeigen der aktiven Paketfilter-Regelliste

Iem folgenden Beispiel wird die Ausgabe der aktiven, in den Kernel geladenen Paketfilter-Regelliste gezeigt.

```
# ipfstat -io
empty list for ipfilter(out)
pass in quick on dmfe1 from 192.168.1.0/24 to any
pass in all
block in on dmfe1 from 192.168.1.10/32 to any
```

▼ So zeigen Sie die inaktive Paketfilter-Regelliste an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Zeigen Sie die inaktive Paketfilter-Regelliste an.**

   ```
   # ipfstat -I -io
   ```

Beispiel 26–3 Anzeigen der inaktiven Paketfilter-Regelliste

Im folgenden Beispiel wird die Ausgabe der inaktiven Paketfilter-Regelliste gezeigt.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
```

▼ So aktivieren Sie eine andere oder aktualisierte Paketfilter-Regelliste

Verwenden Sie das folgende Verfahren, wenn Sie eine der folgenden Aufgaben durchführen möchten:

- Aktivieren einer anderen Paketfilter-Regelliste als der, die derzeit von Oracle Solaris IP Filter verwendet wird.
- Neuladen einer aktualisierten Paketfilter-Regelliste.

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Führen Sie einen der folgenden Schritte aus:**

- Erstellen Sie eine neue Regelliste in einer separaten Datei Ihrer Wahl, wenn Sie eine vollständig andere Regelliste aktivieren möchten.
- Aktualisieren Sie die aktuelle Regelliste, indem Sie die Konfigurationsdatei bearbeiten, in der die Regelliste enthalten ist.

3. **Entfernen Sie die aktuelle Regelliste und laden Sie eine neue.**

   `# ipf -Fa -f` *filename*

   Der *Dateiname* kann entweder der Name einer neuen Datei mit der neuen Regelliste oder der Name einer aktualisierten Datei sein, die die aktive Regelliste enthält.

   Die aktive Regelliste wird aus dem Kernel entfernt. Die Regeln in der Datei *Dateiname* werden zur aktiven Regelliste.

Hinweis – Sie müssen diesen Befehl auch dann eingeben, wenn Sie die aktuelle Konfigurationsdatei neu laden. Andernfalls bleibt die alte Regelliste aktiviert, und die geänderte Regelliste in der aktualisierten Konfigurationsdatei wird nicht übernommen.

Verwenden Sie keine Befehle wie `ipf -D` oder `svcadm restart`, um die aktualisierte Regelliste zu laden. Diese Befehle legen Ihr Netzwerk offen, da sie die Firewall vor dem Laden der neuen Regelliste deaktivieren.

Beispiel 26–4 Aktivieren einer anderen Paketfilter-Regelliste

Im folgenden Beispiel wird gezeigt, wie Sie eine Paketfilter-Regelliste durch eine andere Liste in einer separaten Konfigurationsdatei (`/etc/ipf/ipf.conf`) ersetzen.

```
# ipfstat -io
empty list for ipfilter(out)
pass in quick on dmfe all
# ipf -Fa -f /etc/ipf/ipf.conf
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
```

Beispiel 26–5 Neuladen einer aktualisierten Paketfilter-Regelliste

Im folgenden Beispiel wird gezeigt, wie Sie eine derzeit aktive und aktualisierte Paketfilter-Regelliste neu laden. Die in diesem Beispiel verwendete Datei heißt `/etc/ipf/ipf.conf`.

```
# ipfstat -io (Optional)
empty list for ipfilter (out)
block in log quick from 10.0.0.0/8 to any

(Edit the /etc/ipf/ipf.conf configuration file.)
```

```
# ip -Fa -f /etc/ipf/ipf.conf
# ipfstat -io (Optional)
empty list for ipfilter (out)
block in log quick from 10.0.0.0/8 to any
block in quick on elx10 from 192.168.0.0/12 to any
```

▼ So entfernen Sie eine Paketfilter-Regelliste

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Entfernen Sie die Regelliste.**

   ```
   # ipf -F [a|i|o]
   ```

   `-a` Entfernt alle Filterregeln aus der Regelliste.

   `-i` Entfernt alle Filterregeln für eingehende Pakete.

   `-o` Entfernt alle Filterregeln für abgehende Pakete.

Beispiel 26–6 Entfernen einer Paketfilter-Regelliste

Im folgenden Beispiel wird gezeigt, wie Sie alle Filterregeln aus der aktiven Paketfilter-Regelliste entfernen.

```
# ipfstat -io
block out log on dmf0 all
block in log quick from 10.0.0.0/8 to any
# ipf -Fa
# ipfstat -io
empty list for ipfilter(out)
empty list for ipfilter(in)
```

▼ So fügen Sie der aktiven Paketfilter-Regelliste Regeln hinzu

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Wählen Sie eine der folgenden Methoden, um der aktiven Regelliste Regeln hinzuzufügen:**

- Fügen Sie die Regeln über eine Befehlszeile mithilfe des Befehls `ipf -f -` zur Regelliste hinzu.

  ```
  # echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
  ```
- Führen Sie einen der folgenden Befehle aus:

  a. Erstellen Sie eine Regelliste in einer Datei Ihrer Wahl.

  b. Fügen Sie die von Ihnen erstellten Regeln zur aktiven Regelliste hinzu.

  ```
  # ipf -f filename
  ```

  Die Regeln in der Datei *Dateiname* werden am Ende der aktiven Regelliste eingefügt. Da Solaris IP Filter den „last matching rule“-Algorithmus verwendet, legen die hinzugefügten Regeln die Filterprioritäten fest, es sei denn, sie verwenden das Schlüsselwort `quick`. Wenn ein Paket einer Regel entspricht, die das Schlüsselwort `quick` enthält, wird die Aktion für diese Regel ausgeführt und alle weiteren Regeln werden ignoriert.

Beispiel 26–7 Anhängen von Regeln an die aktive Paketfilter-Regelliste

Im folgenden Beispiel wird gezeigt, wie Sie eine Regel über die Befehlszeile an die aktive Paketfilter-Regelliste anhängen.

```
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
# echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
```

▼ So fügen Sie der inaktiven Paketfilter-Regelliste Regeln hinzu

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Erstellen Sie eine Regelliste in einer Datei Ihrer Wahl.**

3. **Fügen Sie die von Ihnen erstellten Regeln zur inaktiven Regelliste hinzu.**

   ```
   # ipf -I -f filename
   ```

   Die Regeln in der Datei *Dateiname* werden am Ende der inaktiven Regelliste eingefügt. Da Solaris IP Filter den „last matching rule“-Algorithmus verwendet, legen die hinzugefügten

Regeln die Filterprioritäten fest, es sei denn, sie verwenden das Schlüsselwort `quick.` Wenn ein Paket einer Regel entspricht, die das Schlüsselwort `quick` enthält, wird die Aktion für diese Regel ausgeführt und alle weiteren Regeln werden ignoriert.

Beispiel 26–8 Anhängen von Regeln an die interaktive Regelliste

Im folgenden Beispiel wird gezeigt, wie Sie eine Regel aus einer Datei zur inaktiven Paketfilter-Regelliste hinzufügen.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
# ipf -I -f /etc/ipf/ipf.conf
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
```

▼ So wechseln Sie zwischen der aktiven und der inaktiven Paketfilter-Regelliste

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Wechseln Sie von der aktiven zur inaktiven Paketfilter-Regelliste.**

   ```
   # ipf -s
   ```

   Mit diesem Befehl können Sie zwischen der aktiven und der inaktiven Paketfilter-Regelliste im Kernel wechseln. Falls die inaktive Regelliste leer ist, findet keine Paketfilterung statt.

Beispiel 26–9 Wechseln zwischen der aktiven und der inaktiven Paketfilter-Regelliste

Im folgenden Beispiel wird gezeigt, wie Sie mit dem Befehl `ipf -s` die inaktive Regelliste zur aktiven Regelliste machen und die aktive Regelliste zur inaktiven.

- Bevor Sie den Befehl `ipf -s` ausführen, zeigt die Ausgabe des Befehls `ipfstat -I -io` die Regeln in der inaktiven Regelliste an. Die Ausgabe des Befehls `ipfstat - io` zeigt die Regeln in der aktiven Regelliste an.

  ```
  # ipfstat -io
  empty list for ipfilter(out)
  block in log quick from 10.0.0.0/8 to any
  block in on dmfe1 proto tcp from 10.1.1.1/32 to any
  # ipfstat -I -io
  ```

```
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
```

- Nach dem Ausführen des Befehls `ipf -s` zeigt die Ausgabe der Befehle `ipfstat -I -io` und `ipfstat -io` die Inhalte der zwei gewechselten Regellisten an.

```
# ipf -s
Set 1 now inactive
# ipfstat -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
# ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
```

So entfernen Sie eine inaktive Paketfilter-Regelliste aus dem Kernel

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Geben Sie die inaktive Regelliste im Befehl „flush all“ an.**

   ```
   # ipf -I -Fa
   ```

   Mit diesem Befehl entfernen Sie die inaktive Paketfilter-Regelliste aus dem Kernel.

Hinweis – Wenn Sie anschließend den Befehl `ipf -s` ausführen, wird die leere inaktive Regelliste zur aktiven Regelliste. Eine leere aktive Regelliste bedeutet, dass *keine* Filterung durchgeführt wird.

Beispiel 26–10 Löschen einer inaktiven Paketfilter-Regelliste aus dem Kernel

Im folgenden Beispiel wird gezeigt, wie Sie die in aktive Paketfilter-Regelliste entfernen, so dass keine Regeln angewendet werden.

```
# ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
# ipf -I -Fa
# ipfstat -I -io
empty list for inactive ipfilter(out)
empty list for inactive ipfilter(in)
```

Verwalten der NAT-Regeln für Oracle Solaris IP Filter

Zum Verwalten, Anzeigen und Ändern der NAT-Regeln verwenden Sie die folgenden Verfahren.

▼ So zeigen Sie die aktiven NAT-Regeln an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Zeigen Sie die aktiven NAT-Regeln an.**

```
# ipnat -l
```

Beispiel 26–11 Anzeigen der aktiven NAT-Regeln

Im folgenden Beispiel wird die Ausgabe der aktiven NAT-Regelliste gezeigt.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

▼ So entfernen Sie NAT-Regeln

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Entfernen Sie die aktuellen NAT-Regeln.**

```
# ipnat -C
```

Beispiel 26–12 Entfernen der NAT-Regeln

Im folgenden Beispiel wird gezeigt, wie Sie die Einträge aus der aktuellen NAT-Regelliste entfernen.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
# ipnat -C
1 entries flushed from NAT list
# ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
```

So hängen Sie Regeln an die NAT-Regelliste an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Wählen Sie eine der folgenden Methoden, um der aktiven Regelliste Regeln hinzuzufügen:**

   - Fügen Sie die Regeln über eine Befehlszeile mithilfe des Befehls `ipnat -f -` zur NAT-Regelliste hinzu.

     ```
     # echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
     ```

   - Führen Sie einen der folgenden Befehle aus:

     a. Erstellen Sie eine NAT-Regelliste in einer Datei Ihrer Wahl.

     b. Fügen Sie die von Ihnen erstellten Regeln zur aktiven NAT-Regelliste hinzu.

        ```
        # ipnat -f filename
        ```

        Die Regeln in der Datei *Dateiname* werden am Ende der NAT-Regelliste eingefügt.

Beispiel 26–13 Anhängen von Regeln an die NAT-Regelliste

Im folgenden Beispiel wird gezeigt, wie Sie eine Regel über die Befehlszeile an die aktive NAT-Regelliste anhängen.

```
# ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
# echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

Verwalten der Adresspools für Oracle Solaris IP Filter

Zum Verwalten, Anzeigen und Ändern der Adresspools verwenden Sie die folgenden Verfahren.

▼ So zeigen Sie die aktiven Adresspools an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Zeigen Sie den aktiven Adresspool an.**

   ```
   # ippool -l
   ```

Beispiel 26–14 Anzeigen des aktiven Adresspools

Im folgenden Beispiel wird gezeigt, wie Sie den Inhalt des aktiven Adresspools anzeigen.

```
# ippool -l
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

▼ So entfernen Sie einen Adresspool

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Entfernen Sie die Einträge aus dem aktuellen Adresspool.**

   ```
   # ippool -F
   ```

Beispiel 26–15 Entfernen eines Adresspools

Im folgenden Beispiel wird gezeigt, wie Sie einen Adresspool entfernen.

```
# ippool -l
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
# ippool -F
```

```
1 object flushed
# ippool -l
```

So hängen Sie Regeln an einen Adresspool an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Wählen Sie eine der folgenden Methoden, um der aktiven Regelliste Regeln hinzuzufügen:**

   - Fügen Sie die Regeln über eine Befehlszeile mithilfe des Befehls `ippool -f -` zur Regelliste hinzu.

     ```
     # echo "table role = ipf type = tree number = 13
     {10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24};" | ippool -f -
     ```

   - Führen Sie einen der folgenden Befehle aus:

     a. Erstellen Sie einen zusätzlichen Adresspool in einer Datei Ihrer Wahl.

     b. Fügen Sie die von Ihnen erstellten Regeln zum aktiven Adresspool hinzu.

     ```
     # ippool -f filename
     ```

     Die Regeln in der Datei *Dateiname* werden am Ende des aktiven Adresspools eingefügt.

Beispiel 26–16 Anhängen von Regeln an einen Adresspool

Im folgenden Beispiel wird gezeigt, wie Sie einen Adresspool über die Befehlszeile zur aktuellen Adresspool-Regelliste hinzufügen.

```
# ippool -l
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
# echo "table role = ipf type = tree number = 100
 {10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24};" | ippool -f -
# ippool -l
table role = ipf type = tree number = 100
        { 10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24; };
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

Anzeigen von Statistiken und Informationen zu Oracle Solaris IP Filter

TABELLE 26–5 Anzeigen von Statistiken und Informationen zu Oracle Solaris IP Filter (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Anzeigen der Statustabellen.	Zeigen Sie die Statustabellen an, um Informationen zur Paketfilterung mit dem Befehl `ipfstat` zu beziehen.	„So zeigen Sie die Statustabellen für Oracle Solaris IP Filter an" auf Seite 707
Anzeigen der Statusstatistiken.	Zeigen Sie die Statistiken zu dem Paket-Statusinformationen mit dem Befehl `ipfstat - s` an.	„So zeigen Sie die Statusstatistiken für Oracle Solaris IP Filter an" auf Seite 708
Anzeigen der NAT-Statistiken.	Zeigen Sie die NAT-Statistiken mit dem Befehl `ipnat -s` an.	„So zeigen Sie die NAT-Statistiken für Oracle Solaris IP Filter an" auf Seite 709
Anzeigen der Adresspool-Statistiken.	Zeigen Sie die Adresspool-Statistiken mit dem Befehl `ippool -s` an.	„So zeigen Sie die Adresspool-Statistiken für Oracle Solaris IP Filter an" auf Seite 709

▼ So zeigen Sie die Statustabellen für Oracle Solaris IP Filter an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services* .

2. **Zeigen Sie die Statustabelle an.**

```
# ipfstat
```

Hinweis – Mit der Option `-t` können Sie die Statustabelle im Top Utility-Format anzeigen.

Beispiel 26–17 Anzeigen der Statustabellen für Oracle Solaris IP Filter

Im folgenden Beispiel wird gezeigt, wie eine Statustabelle angezeigt wird.

```
# ipfstat
bad packets:            in 0    out 0
 input packets:         blocked 160 passed 11 nomatch 1 counted 0 short 0
output packets:         blocked 0 passed 13681 nomatch 6844 counted 0 short 0
 input packets logged:  blocked 0 passed 0
output packets logged:  blocked 0 passed 0
 packets logged:        input 0 output 0
 log failures:          input 0 output 0
fragment state(in):     kept 0  lost 0
fragment state(out):    kept 0  lost 0
packet state(in):       kept 0  lost 0
packet state(out):      kept 0  lost 0
ICMP replies:   0       TCP RSTs sent:  0
Invalid source(in):     0
Result cache hits(in):  152     (out):  6837
IN Pullups succeeded:   0       failed: 0
OUT Pullups succeeded:  0       failed: 0
Fastroute successes:    0       failures:       0
TCP cksum fails(in):    0       (out):  0
IPF Ticks:      14341469
Packet log flags set: (0)
        none
```

So zeigen Sie die Statusstatistiken für Oracle Solaris IP Filter an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

2. **Zeigen Sie die Statusstatistiken an.**

```
# ipfstat -s
```

Beispiel 26–18 Anzeigen der Statusstatistiken für Oracle Solaris IP Filter

Im folgenden Beispiel wird gezeigt, wie die Statusstatistiken angezeigt werden.

```
# ipfstat -s
IP states added:
        0 TCP
        0 UDP
        0 ICMP
        0 hits
        0 misses
        0 maximum
        0 no memory
        0 max bucket
        0 active
```

```
        0 expired
        0 closed
State logging enabled

State table bucket statistics:
        0 in use
        0.00% bucket usage
        0 minimal length
        0 maximal length
        0.000 average length
```

So zeigen Sie die NAT-Statistiken für Oracle Solaris IP Filter an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

2. **Anzeigen der NAT-Statistiken.**

   ```
   # ipnat -s
   ```

Beispiel 26–19 Anzeigen der NAT-Statistiken für Oracle Solaris IP Filter

Im folgenden Beispiel wird gezeigt, wie die NAT-Statistiken angezeigt werden.

```
# ipnat -s
mapped  in      0       out     0
added   0       expired 0
no memory       0       bad nat 0
inuse   0
rules   1
wilds   0
```

So zeigen Sie die Adresspool-Statistiken für Oracle Solaris IP Filter an

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

2 Anzeigen der Adresspool-Statistiken.

```
# ippool -s
```

Beispiel 26–20 Anzeigen der Adresspool-Statistiken für Oracle Solaris IP Filter

Im folgenden Beispiel wird gezeigt, wie die Adresspool-Statistiken angezeigt werden.

```
# ippool -s
Pools:  3
Hash Tables:    0
Nodes:  0
```

Arbeiten mit Protokolldateien für Oracle Solaris IP Filter

TABELLE 26–6 Arbeiten mit Protokolldateien für Oracle Solaris IP Filter (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Erstellen einer Protokolldatei.	Erstellen Sie eine separate Oracle Solaris IP Filter-Protokolldatei.	„So richten Sie eine Protokolldatei für Oracle Solaris IP Filter ein" auf Seite 710
Anzeigen der Protokolldateien.	Zeigen Sie die Status-, NAT- und der normalen Protokolldateien mithilfe des Befehls `ipmon` an.	„So zeigen Sie Oracle Solaris IP Filter-Protokolldateien an" auf Seite 711
Leeren des Paketprotokollpuffers.	Löschen Sie den Inhalt aus dem Paketprotokollpuffer mithilfe des Befehls `ipmon - F`.	„So leeren Sie die Paketprotokolldatei" auf Seite 713
Speichern der protokollierten Pakete in einer Datei.	Speichern Sie die protokollierten Pakete in einer Datei, so dass später darauf zugegriffen werden kann.	„So speichern Sie protokollierte Pakete in einer Datei" auf Seite 713

▼ So richten Sie eine Protokolldatei für Oracle Solaris IP Filter ein

In der Standardeinstellung werden alle Informationen für Oracle Solaris IP Filter in der Datei `syslogd` protokolliert. Richten Sie eine Protokolldatei ein, um Oracle Solaris IP Filter-Verkehrsinformationen getrennt von anderen Daten aufzuzeichnen, die in der Standard-Protokolldatei aufgezeichnet werden. Führen Sie die folgenden Schritte aus.

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

2. **Fügen Sie der Datei** `/etc/syslog.conf` **die beiden folgenden Zeilen hinzu:**

   ```
   # Save IPFilter log output to its own file
   local0.debug             /var/log/log-name
   ```

   Hinweis – Achten Sie in der zweiten Zeile darauf, die Tabulatortaste und nicht die Leertaste zum Trennen von `local0.debug` und `/var/log/`*Protokollname* zu verwenden.

   ---

3. **Erstellen Sie die neue Protokolldatei.**

   ```
   # touch /var/log/log-name
   ```

4. **Starten Sie den system-log-Service neu.**

   ```
   # svcadm restart system-log
   ```

Beispiel 26–21 Erstellen eines Oracle Solaris IP Filter-Protokolls

Im folgenden Beispiel wird gezeigt, wie Sie die Datei `ipmon.log` anlegen, um IP-Filterinformationen zu archivieren.

Unter `/etc/syslog.conf`:

```
# Save IPFilter log output to its own file
local0.debug             /var/log/ipmon.log
```

An der Befehlszeile:

```
# touch /var/log/ipmon.log
# svcadm restart system-log
```

▼ So zeigen Sie Oracle Solaris IP Filter-Protokolldateien an

Bevor Sie beginnen Zum Aufzeichnen der Oracle Solaris IP Filter-Daten sollten Sie eine separate Protokolldatei erstellen. Näheres dazu finden Sie unter „So richten Sie eine Protokolldatei für Oracle Solaris IP Filter ein“ auf Seite 710.

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

2. **Zeigen Sie die Status-, NAT- oder normalen Protokolldateien an. Zum Anzeigen einer Protokolldatei geben Sie den folgenden Befehl mit der entsprechenden Option an:**

   `# ipmon -o [S|N|I]` *filename*

   `S` Zeigt die Status-Protokolldatei an.

   `N` Zeigt die NAT-Protokolldatei an.

   `I` Zeigt die normale IP-Protokolldatei an.

   Um alle Status-, NAT- und die normalen Protokolldateien anzuzeigen, geben Sie alle Optionen an:

   `# ipmon -o SNI` *filename*

   - **Vorausgesetzt, Sie stoppen zunächst manuell den `ipmon`-Daemon, können Sie auch den folgenden Befehl zum Anzeigen der Status-, NAT- und Oracle Solaris IP Filter-Protokolldateien verwenden:**

     `# ipmon -a` *filename*

     Hinweis – Rufen Sie den Befehl `ipmon -a` nicht auf, so lange der `ipmon`-Daemon noch ausgeführt wird. In der Regel wird der Daemon beim Booten des Systems automatisch gestartet. Mit dem Befehl `ipmon -a` öffnen Sie darüber hinaus eine weitere Kopie von `ipmon`. In diesem Fall lesen beide Kopien die gleichen Protokollinformationen, aber nur eine erhält eine bestimmte Protokolldatei.

   Weitere Informationen zum Anzeigen von Protokolldateien finden Sie in der Manpage `ipmon(1M)`.

Beispiel 26–22 Anzeigen von Oracle Solaris IP Filter-Protokolldateien

Im folgenden Beispiel wird die Ausgabe von `/var/ipmon.log` gezeigt.

```
# ipmon -o SNI /var/ipmon.log
02/09/2004 15:27:20.606626 hme0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

oder

```
# pkill ipmon
# ipmon -aD /var/ipmon.log
02/09/2004 15:27:20.606626 hme0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

▼ So leeren Sie die Paketprotokolldatei

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

2. **Leeren Sie den Paketprotokollpuffer.**

   ```
   # ipmon -F
   ```

Beispiel 26–23 Leeren der Paketprotokolldatei

Im folgenden Beispiel wird die Ausgabe gezeigt, wenn eine Protokolldatei entfernt wird. Das System erstellt auch dann einen Bericht, wenn nichts in der Protokolldatei gespeichert ist; wie in diesem Beispiel.

```
# ipmon -F
0 bytes flushed from log buffer
0 bytes flushed from log buffer
0 bytes flushed from log buffer
```

▼ So speichern Sie protokollierte Pakete in einer Datei

1. **Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.**

   Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services* .

2. **Speichern Sie die protokollierten Pakete in einer Datei.**

   ```
   # cat /dev/ipl > filename
   ```

   Setzen Sie die Protokollierung von Paketen in die Datei *Dateiname* fort, bis Sie den Vorgang durch Drücken von `Strg-C` unterbrechen, um zur Befehlszeile zu gelangen.

Beispiel 26–24 Speichern von protokollierten Paketen in einer Datei

Im folgenden Beispiel wird die Ausgabe gezeigt, wenn protokollierte Pakete in einer Datei gespeichert werden.

```
# cat /dev/ipl > /tmp/logfile
^C#

# ipmon -f /tmp/logfile
02/09/2004 15:30:28.708294 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 52 -S IN
02/09/2004 15:30:28.708708 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.792611 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 70 -AP IN
02/09/2004 15:30:28.872000 hme0 @0:1 p 129.146.157.149,33923 ->
 129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872142 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 43 -AP IN
02/09/2004 15:30:28.872808 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872951 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 47 -AP IN
02/09/2004 15:30:28.926792 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
.
.
(output truncated)
```

Erstellen und Bearbeiten von Konfigurationsdateien für Oracle Solaris IP Filter

Zum Erstellen oder Ändern von Regellisten und Adresspools müssen Sie die Konfigurationsdateien direkt bearbeiten. Die Konfigurationsdateien werden nach den Standardregeln zur UNIX-Syntax erstellt:

- Das Nummernzeichen (#) kennzeichnet eine Zeile als einen Kommentar.
- Regeln und Kommentare können auf der gleichen Zeile vorhanden sein.
- Zusätzliche Leerzeichen sind zulässig, um die Lesbarkeit von Regeln zu erhöhen.
- Regeln können mehrere Zeilen umfassen. Geben Sie einen umgekehrten Schrägstich (\) am Ende einer Zeile ein, um zu kennzeichnen, dass die Regel auf der nächsten Zeile fortgesetzt wird.

▼ So erstellen Sie eine Konfigurationsdatei für Oracle Solaris IP Filter

Im folgenden Verfahren wird beschrieben, wie Sie Folgendes einrichten:

- Konfigurationsdateien zur Paketfilterung
- Konfigurationsdateien für NAT-Regeln
- Konfigurationsdateien für Adresspools

1 Nehmen Sie eine Rolle an, die das IP Filter Management-Rechteprofil umfasst, oder melden Sie sich als Superuser an.

Sie können das IP Filter Management-Rechteprofil einer von Ihnen erstellten Rolle zuweisen. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services* .

2 Starten Sie einen Dateieditor Ihrer Wahl. Erstellen oder bearbeiten Sie die Konfigurationsdateien für die Funktion, die Sie konfigurieren möchten.

- Zum Erstellen einer Konfigurationsdatei für Paketfilterregeln bearbeiten Sie die Datei `ipf.conf`.

  Oracle Solaris IP Filter verwendet die Paketfilterregeln in der Datei `ipf.conf.` Wenn Sie die Paketfilterregeln in der Datei `/etc/ipf/ipf.conf` angeben, wird diese Datei beim Booten des Systems geladen. Sollen die Filterregeln nicht beim Booten geladen werden, speichern Sie die Datei in einem beliebigen anderen Verzeichnis. Sie können die Regeln dann gemäß der Beschreibung unter „So aktivieren Sie eine andere oder aktualisierte Paketfilter-Regelliste" auf Seite 697 mit dem Befehl `ipf` aktivieren.

  Informationen zum Erstellen der Paketfilterregeln finden Sie unter „Verwenden der Paketfilter-Funktionen in Oracle Solaris IP Filter" auf Seite 671.

  Hinweis – Ist die Datei `ipf.conf` leer, findet keine Filterung statt. Eine leere `ipf.conf`-Datei verhält sich wie eine Regelliste mit dem folgenden Inhalt:

  ```
  pass in all
  pass out all
  ```

- Zum Erstellen einer Konfigurationsdatei für NAT-Regeln bearbeiten Sie die Datei `ipnat.conf`.

  Oracle Solaris IP Filter verwendet die NAT-Regeln in der Datei `ipnat.conf.` Wenn Sie die NAT-Regeln in der Datei `/etc/ipf/ipnat.conf` angeben, wird diese Datei beim Booten des Systems geladen. Sollen die NAT-Regeln nicht während des Bootens geladen werden, Datei `ipnat.conf` in einem beliebigen anderen Verzeichnis. Sie können die NAT-Regeln dann mit dem Befehl `ipnat` aktivieren.

Informationen zum Erstellen der NAT-Regeln finden Sie unter „Verwenden der NAT-Funktion in Oracle Solaris IP Filter“ auf Seite 674.

- Zum Erstellen einer Konfigurationsdatei für Adresspools bearbeiten Sie die Datei `ippool.conf`.

  Oracle Solaris IP Filter verwendet den Adresspool in der Datei `ippool.conf.` Wenn Sie die Adresspool-Regeln in der Datei `/etc/ipf/ippool.conf` angeben, wird diese Datei beim Booten geladen. Soll der Adresspool nicht beim Booten geladen werden, speichern Sie die Datei`ippool.conf` in einem beliebigen anderen Verzeichnis. Sie können den Adresspool dann mit dem Befehl `ippool` aktivieren.

  Informationen zum Erstellen von Adresspools finden Sie unter „Verwenden der Adresspool-Funktion in Oracle Solaris IP Filter“ auf Seite 675.

Beispiel für Oracle Solaris IP Filter-Konfigurationsdateien

Die folgenden Beispiele verdeutlichen die Anwendung von Paketfilterregeln in Paketfilterkonfigurationen.

BEISPIEL 26–25 Oracle Solaris IP Filter-Hostkonfiguration

In diesem Beispiel wird eine Konfiguration auf einem Host-Computer mit der Netzwerkschnittstelle `elxl` gezeigt.

```
# pass and log everything by default
pass in log on elxl0 all
pass out log on elxl0 all

# block, but don't log, incoming packets from other reserved addresses
block in quick on elxl0 from 10.0.0.0/8 to any
block in quick on elxl0 from 172.16.0.0/12 to any

# block and log untrusted internal IPs. 0/32 is notation that replaces
# address of the machine running Solaris IP Filter.
block in log quick from 192.168.1.15 to <thishost>
block in log quick from 192.168.1.43 to <thishost>

# block and log X11 (port 6000) and remote procedure call
# and portmapper (port 111) attempts
block in log quick on elxl0 proto tcp from any to elxl0/32 port = 6000 keep state
block in log quick on elxl0 proto tcp/udp from any to elxl0/32 port = 111 keep state
```

Diese Regel beginnt mit zwei nicht eingeschränkten Regeln, die den gesamten über die Schnittstelle `elxl` eingehenden und ausgehenden Verkehr zulassen. Die zweite Regelliste blockiert die eingehenden Pakete von den privaten Adressbereichen `10.0.0.0` und `172.16.0.0` und verhindert deren Eintritt in die Firewall. Die nächste Regelliste blockiert bestimmte interne Adressen vom Host-Computer. Abschließend blockiert die letzte Regelliste Pakete, die an Port

BEISPIEL 26–25 Oracle Solaris IP Filter-Hostkonfiguration *(Fortsetzung)*

6000 und Port 111 eingehen.

BEISPIEL 26–26 Oracle Solaris IP Filter-Serverkonfiguration

In diesem Beispiel wird die Konfiguration für einen Host-Computer gezeigt, der als Webserver arbeitet. Dieser Computer verfügt über die Netzwerkschnittstelle `eri`.

```
# web server with an eri interface
# block and log everything by default; then allow specific services
# group 100 - inbound rules
# group 200 - outbound rules
# (0/32) resolves to our IP address)
*** FTP proxy ***


# block short packets which are packets fragmented too short to be real.
block in log quick all with short


# block and log inbound and outbound by default, group by destination
block in log on eri0 from any to any head 100
block out log on eri0 from any to any head 200


# web rules that get hit most often
pass in quick on eri0 proto tcp from any \
to eri0/32 port = http flags S keep state group 100
pass in quick on eri0 proto tcp from any \
to eri0/32 port = https flags S keep state group 100


# inbound traffic - ssh, auth
pass in quick on eri0 proto tcp from any \
to eri0/32 port = 22 flags S keep state group 100
pass in log quick on eri0 proto tcp from any \
to eri0/32 port = 113 flags S keep state group 100
pass in log quick on eri0 proto tcp from any port = 113 \
to eri0/32 flags S keep state group 100


# outbound traffic - DNS, auth, NTP, ssh, WWW, smtp
pass out quick on eri0 proto tcp/udp from eri0/32 \
to any port = domain flags S keep state group 200
pass in quick on eri0 proto udp from any port = domain to eri0/32 group 100

pass out quick on eri0 proto tcp from eri0/32 \
to any port = 113 flags S keep state group 200
pass out quick on eri0 proto tcp from eri0/32 port = 113 \
to any flags S keep state group 200

pass out quick on eri0 proto udp from eri0/32 to any port = ntp group 200
pass in quick on eri0 proto udp from any port = ntp to eri0/32 port = ntp group 100

pass out quick on eri0 proto tcp from eri0/32 \
```

BEISPIEL 26–26 Oracle Solaris IP Filter-Serverkonfiguration *(Fortsetzung)*

```
to any port = ssh flags S keep state group 200

pass out quick on eri0 proto tcp from eri0/32 \
to any port = http flags S keep state group 200
pass out quick on eri0 proto tcp from eri0/32 \
to any port = https flags S keep state group 200

pass out quick on eri0 proto tcp from eri0/32 \
to any port = smtp flags S keep state group 200


# pass icmp packets in and out
pass in quick on eri0 proto icmp from any to eri0/32  keep state group 100
pass out quick on eri0 proto icmp from eri0/32 to any keep state group 200


# block and ignore NETBIOS packets
block in quick on eri0 proto tcp from any \
to any port = 135 flags S keep state group 100

block in quick on eri0 proto tcp from any port = 137 \
to any flags S keep state group 100
block in quick on eri0 proto udp from any to any port = 137 group 100
block in quick on eri0 proto udp from any port = 137 to any group 100

block in quick on eri0 proto tcp from any port = 138 \
to any flags S keep state group 100
block in quick on eri0 proto udp from any port = 138 to any group 100

block in quick on eri0 proto tcp from any port = 139 to any flags S keep state
group 100
block in quick on eri0 proto udp from any port = 139 to any group 100
```

BEISPIEL 26–27 Oracle Solaris IP Filter-Routerkonfiguration

Das folgende Beispiel zeigt eine Konfiguration für einen Router, der über eine interne Schnittstelle `ce0` und eine externe Schnittstelle `ce1` verfügt.

```
# internal interface is ce0 at 192.168.1.1
# external interface is ce1 IP obtained via DHCP
# block all packets and allow specific services
*** NAT ***
*** POOLS ***


# Short packets which are fragmented too short to be real.
block in log quick all with short


# By default, block and log everything.
block in log on ce0 all
block in log on ce1 all
block out log on ce0 all
block out log on ce1 all
```

BEISPIEL 26–27 Oracle Solaris IP Filter-Routerkonfiguration *(Fortsetzung)*

```
# Packets going in/out of network interfaces that aren't on the loopback
# interface should not exist.
block in log quick on ce0 from 127.0.0.0/8 to any
block in log quick on ce0 from any to 127.0.0.0/8
block in log quick on ce1 from 127.0.0.0/8 to any
block in log quick on ce1 from any to 127.0.0.0/8


# Deny reserved addresses.
block in quick on ce1 from 10.0.0.0/8 to any
block in quick on ce1 from 172.16.0.0/12 to any
block in log quick on ce1 from 192.168.1.0/24 to any
block in quick on ce1 from 192.168.0.0/16 to any


# Allow internal traffic
pass in quick on ce0 from 192.168.1.0/24 to 192.168.1.0/24
pass out quick on ce0 from 192.168.1.0/24 to 192.168.1.0/24


# Allow outgoing DNS requests from our servers on .1, .2, and .3
pass out quick on ce1 proto tcp/udp from ce1/32 to any port = domain keep state
pass in quick on ce0 proto tcp/udp from 192.168.1.2 to any port = domain keep state
pass in quick on ce0 proto tcp/udp from 192.168.1.3 to any port = domain keep state


# Allow NTP from any internal hosts to any external NTP server.
pass in quick on ce0 proto udp from 192.168.1.0/24 to any port = 123 keep state
pass out quick on ce1 proto udp from any to any port = 123 keep state


# Allow incoming mail
pass in quick on ce1 proto tcp from any to ce1/32 port = smtp keep state
pass in quick on ce1 proto tcp from any to ce1/32 port = smtp keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = smtp keep state


# Allow outgoing connections: SSH, WWW, NNTP, mail, whois
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 22 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 22 keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 443 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 443 keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = nntp keep state
block in quick on ce1 proto tcp from any to any port = nntp keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = nntp keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = smtp keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = whois keep state
```

BEISPIEL 26–27 Oracle Solaris IP Filter-Routerkonfiguration *(Fortsetzung)*

```
pass out quick on ce1 proto tcp from any to any port = whois keep state


# Allow ssh from offsite
pass in quick on ce1 proto tcp from any to ce1/32 port = 22 keep state


# Allow ping out
pass in quick on ce0 proto icmp all keep state
pass out quick on ce1 proto icmp all keep state


# allow auth out
pass out quick on ce1 proto tcp from ce1/32 to any port = 113 keep state
pass out quick on ce1 proto tcp from ce1/32 port = 113 to any keep state


# return rst for incoming auth
block return-rst in quick on ce1 proto tcp from any to any port = 113 flags S/SA


# log and return reset for any TCP packets with S/SA
block return-rst in log on ce1 proto tcp from any to any flags S/SA


# return ICMP error packets for invalid UDP packets
block return-icmp(net-unr) in proto udp all
```

TEIL V

Mobile IP

Dieser Teil enthält eine Einführung in das Mobile Internet Protocol (Mobile IP) sowie Aufgaben zur Verwaltung von Mobile IP. Sie installieren Mobile IP auf Systemen wie z. B. Laptops und drahtlosen Kommunikationsgeräten, damit diese Computer in fremden Netzwerken betrieben werden können.

Hinweis – Die Mobile IP-Funktion ist in Oracle Solaris-Aktualisierungen nach Solaris 10 8/07 nicht mehr vorhanden.

KAPITEL 27

Mobile IP (Übersicht)

Mobile Internet Protocol (IP) ermöglicht die Übertragung von Informationen zwischen mobilen Computern. *Mobile Computer* sind beispielsweise Laptops und drahtlose Kommunikationsgeräte. Ein mobiler Computer kann seinen Standort zu einem fremden Netzwerk wechseln. Auch in einem solchen Foreign-Netzwerk kann der mobile Computer über das Home-Netzwerk des mobilen Computers kommunizieren. Die Solaris-Implementierung von Mobile IP unterstützt nur IPv4.

Dieses Kapitel enthält die folgenden Informationen:

- „Einführung in Mobile IP" auf Seite 724
- „Mobile IP-Funktionseinheiten" auf Seite 726
- „Arbeitsweise von Mobile IP" auf Seite 726
- „Agent-Erkennung" auf Seite 729
- „Care-of-Adressen" auf Seite 730
- „Mobile IP mit Rücktunnel" auf Seite 731
- „Mobile IP-Registrierung" auf Seite 733
- „Routen von Datagrammen von und an mobile Knoten" auf Seite 738
- „Sicherheitsbetrachtungen für Mobile IP" auf Seite 741

Aufgaben im Zusammenhang mit Mobile IP befinden Sie in Kapitel 28, „Verwalten von Mobile IP (Aufgaben)". Referenzmaterial zu Mobile IP finden Sie in Kapitel 29, „Mobile IP-Dateien und Befehle (Referenz)".

Neuerungen bei Mobile IP

Die Mobile IP-Funktion ist in Solaris 10-Aktualisierungen nach Solaris 10 8/07 nicht mehr vorhanden.

Einführung in Mobile IP

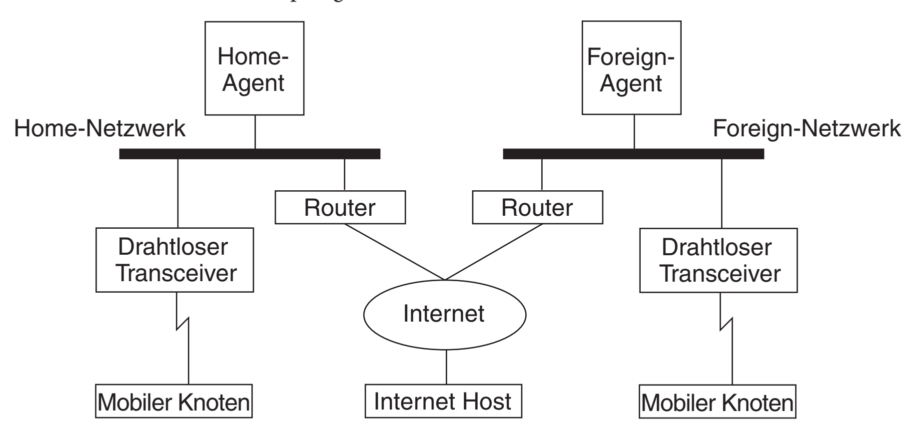
Aktuelle Versionen des Internet Protocol (IP) gehen davon aus, dass der Punkt, an dem ein Computer mit dem Internet oder einem Netzwerk verbunden ist, feststehend ist. Darüber hinaus geht IP davon aus, dass die IP-Adresse eines Computers das Netzwerk angibt, an das der Computer angeschlossen ist. An einen Computer gesendete Datagramme basieren auf den in der IP-Adresse enthaltenen Standortinformationen. Viele Internetprotokolle beruhen darauf, dass die IP-Adresse eines Knotens unverändert bleibt. Wenn eines dieser Protokolle auf einem Mobile IP-Computer ausgeführt wird, schlagen dessen Anwendungen fehl. Selbst HTTP würde fehlschlagen, und sei es nur aufgrund der kurzlebigen TCP-Verbindungen. Das Aktualisieren von IP-Adresse und Webseite stellt keine Belastung dar.

Wird ein mobiler Computer oder, anders gesagt, ein *mobiler Knoten* in ein anderes Netzwerk verschoben und bleibt die IP-Adresse gleich, so spiegelt die Adresse des mobilen Knotens den neuen Anschlusspunkt nicht korrekt wider. Entsprechend können vorhandene Routing-Protokolle Datagramme nicht korrekt zum mobilen Knoten leiten. Der mobile Knoten muss eine neue IP-Adresse erhalten, die den neuen Standort korrekt widerspiegelt. Das Zuweisen einer anderen IP-Adresse ist jedoch recht umständlich. Daher verliert ein mobiler Knoten das Routing, wenn er unter dem aktuellen Internet Protocol ohne eine Änderung seiner Adresse verschoben wird. Ändert der mobile Knoten jedoch seine Adresse, verliert er die Verbindungen.

Die Lösung dieses Problems ist Mobile IP. Mit Mobile IP kann ein mobiler Knoten zwei IP-Adressen verwenden. Die primäre Adresse ist eine feststehende *Home-Adresse*. Die sekundäre Adresse ist eine *Care-Of-Adresse*, die sich mit jedem neuen Anschlusspunkt ändert. Mobile IP gestattet einem Computer freies Roamen im Internet und im Netzwerk einer Organisation, während die gleiche Home-Adresse beibehalten wird. Entsprechend werden bestehende Kommunikationen nicht unterbrochen, wenn der Benutzer den Anschlusspunkt des Computers ändert. Stattdessen wird das Netzwerk mit dem neuen Standort des mobilen Knotens aktualisiert. Definitionen der Begriffe im Zusammenhang mit Mobile IP finden Sie im Glossar.

Die folgende Abbildung zeigt eine allgemeine Mobile IP-Topologie.

ABBILDUNG 27–1 Mobile IP-Topologie



Wenn die in der Abbildung gezeigte Mobile IP-Topologie zu Grunde gelegt wird, zeigt das folgende Szenario, wie sich ein Datagramm von einem Punkt im Mobile IP-Framework zum anderen bewegt:

1. Der Internet-Host sendet unter Angabe der Home-Adresse des mobilen Knotens ein Datagramm an den mobilen Knoten (normaler IP-Routing-Prozess).
2. Befindet sich der mobile Knoten in seinem Home-Netzwerk, wird das Datagramm über den normalen IP-Prozess an den mobilen Knoten zugestellt. Andernfalls erhält der Home-Agent das Datagramm.
3. Befindet sich der mobile Knoten in einem Foreign-Netzwerk, leitete der Home-Agent das Datagramm an den Foreign-Agent weiter. Dazu muss der Home-Agent das Datagramm in ein äußeres Datagramm einkapseln, so dass die IP-Adresse des Foreign-Agent im äußeren IP-Header erscheint.
4. Der Foreign-Agent leitet das Datagramm an den mobilen Knoten weiter.
5. Datagramme vom mobilen Knoten an den Internet-Host werden unter Verwendung der normalen IP-Routing-Verfahren gesendet. Befindet sich der mobile Knoten in einem Foreign-Netzwerk, werden die Pakete an den Foreign-Agent gesendet. Der Foreign-Agent leitet das Datagramm an den Internet-Host weiter.
6. Wenn eine Filterung für eingehende Pakete durchgeführt wird, muss die Quelladresse topologisch korrekt für das Teilnetz sein, aus dem das Datagramm stammt, andernfalls kann der Router das Datagramm nicht weiterleiten. Wenn dieses Szenario für Verbindungen zwischen dem mobilen Knoten und dem korrespondierenden Knoten zutrifft, muss der Foreign-Agent eine Unterstützung für den Rücktunnel bieten. Erst dann kann der Foreign-Agent jedes vom mobilen Knoten gesendete Datagramm an seinen Home-Agent weiterleiten. Der Home-Agent leitet das Datagramm dann über den Pfad weiter, den es genommen hätte, wenn sich der mobile Knoten im Home-Netzwerk befinden würde. Dieser Prozess garantiert, dass die Quelladresse für alle Verbindungen korrekt ist, die das Datagramm durchlaufen muss.

Bei einer drahtlosen Kommunikation zeigt Abbildung 27–1, wie drahtlose Transceiver das Datagramm an den mobilen Knoten übertragen. Darüber hinaus verwenden alle Datagramme zwischen dem Internet-Host und dem mobilen Knoten die Home-Adresse des mobilen Knoten. Die Home-Adresse wird auch dann verwendet, wenn sich der mobile Knoten im Foreign-Netzwerk befindet. Die Care-Of-Adresse wird nur für Kommunikationen mit Mobility-Agents verwendet. Die Care-Of-Adresse ist für den Internet-Host unsichtbar.

Mobile IP-Funktionseinheiten

Mobile IP führt die folgenden neuen Funktionseinheit ein:

- **Mobiler Knoten (Mobile Node, MN)** – Ein Host oder Router, der seinen Anschlusspunkt von einem Netzwerk zu einem anderen ändern und dabei alle vorhandenen Verbindungen mithilfe seiner IP-Home-Adresse beibehalten kann.
- **Home-Agent (HA)** – Ein Router oder Server im Home-Netzwerk eines mobilen Knotens. Der Router fängt Datagramme ab, die an den mobilen Knoten gerichtet sind, und leitet sie an die Care-Of-Adresse weiter. Der Home-Agent pflegt darüber hinaus die aktuellen Informationen zum Standort des mobilen Knotens.
- **Foreign-Agent (FA)** – Ein Router oder Server im Foreign-Netzwerk, das der mobile Knoten besucht. Stellt die Host-Routing-Services für den mobilen Knoten zur Verfügung. Der Foreign-Agent kann darüber hinaus eine Care-Of-Adresse für den mobilen Knoten bereitstellen, solange dieser im Netzwerk registriert ist.

Arbeitsweise von Mobile IP

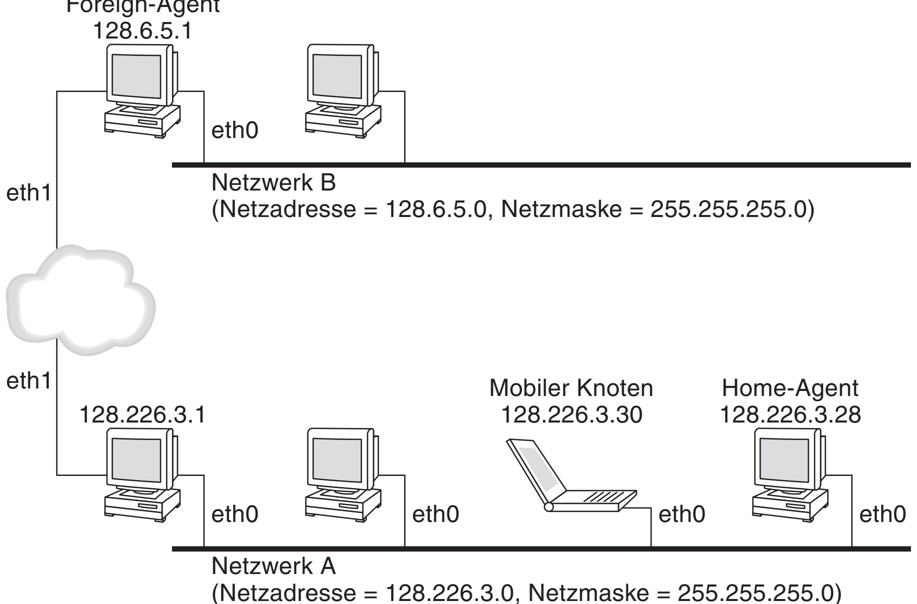
Mobile IP ermöglicht das Routing von IP-Datagrammen an mobile Knoten. Die Home-Adresse des mobilen Knotens identifiziert den mobilen Knoten ungeachtet des Netzwerks, an das er angeschlossen ist. Befindet sich der mobile Knoten nicht in seinem Home-Netzwerk, wird über die Home-Adresse des mobilen Knotens eine Care-Of-Adresse zugewiesen. Die Care-Of-Adresse enthält Informationen zum aktuellen Anschlusspunkt des mobilen Knotens. Mobile IP verwendet einen Registrierungsmechanismus, um die Care-Of-Adresse beim Home-Agent zu registrieren.

Der Home-Agent leitet Datagramme vom Home-Netzwerk an die Care-Of-Adresse weiter. Der Home-Agent konstruiert einen neuen IP-Header, der die Care-Of-Adresse des mobilen Knotens als IP-Zieladresse enthält. Dieser neue Header kapselt das originale IP-Datagramm ein. Entsprechend hat die Home-Adresse des mobilen Knotens keine Auswirkungen auf das Routing eines gekapselten Datagramms, bis das Diagramm an der Care-Of-Adresse eintrifft. Diese Art Kapselung wird als *Tunneling* bezeichnet. Nachdem das Datagramm an der Care-Of-Adresse eingetroffen ist, wird es entkapselt. Dann wird es an den mobilen Knoten zugestellt.

Die folgende Abbildung zeigt einen mobilen Knoten, der sich in seinem Home-Netzwerk (Netzwerk A) befindet. Dann wird der mobile Knoten in ein Foreign-Netzwerk (Netzwerk B)

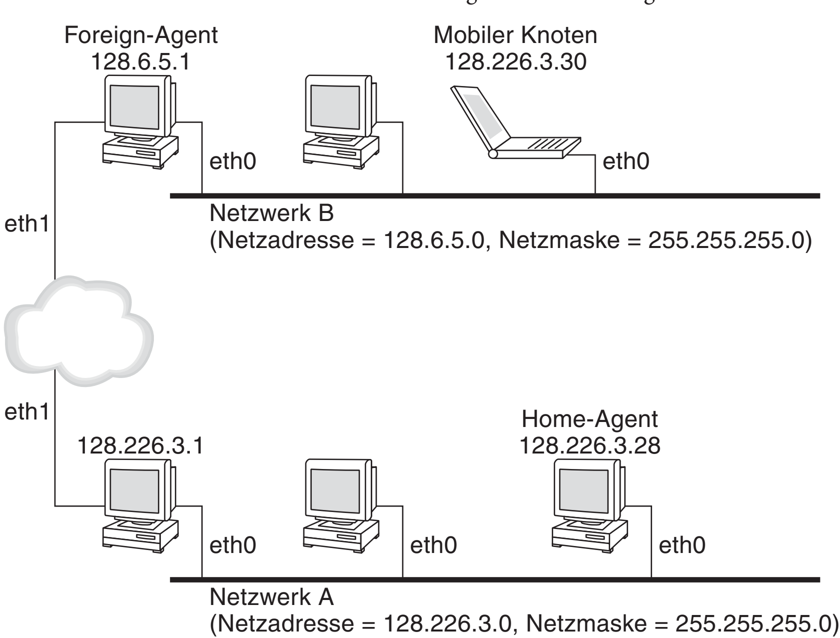
bewegt. Beide Netzwerke unterstützen Mobile IP. Der mobile Knoten ist stets der Home-Adresse des mobilen Knotens (`128.226.3.30`) zugeordnet.

ABBILDUNG 27–2 Mobiler Knoten im Home-Netzwerk



Die folgende Abbildung zeigt einen mobilen Knoten, der in ein Foreign-Netzwerk (Netzwerk B) bewegt wurde. Datagramme für den mobilen Knoten werden vom Home-Agent im Home-Netzwerk (Netzwerk A) abgefangen und gekapselt. Dann werden die Datagramme an den Foreign-Agent im Netzwerk B gesendet. Der Foreign-Agent streift den äußeren Header ab, und das Datagramm an den mobilen Knoten zu, der sich im Netzwerk B befindet.

ABBILDUNG 27–3 Mobiler Knoten wird in ein Foreign-Netzwerk bewegt



Die Care-Of-Adresse kann zu einem Foreign-Agent gehören. Die Care-Of-Adresse kann vom mobilen Knoten über das Dynamic Host Configuration Protocol (DHCP) oder das Point-to-Point Protocol (PPP) bezogen worden sein. Bei Letzteren spricht man davon, dass der mobile Knoten eine co-located Care-Of-Adresse hat (die lokalen Router können nicht unterscheiden, ob der Knoten mobil oder stationär ist).

Mobility-Agents (Home-Agents und Foreign-Agents) geben ihr Vorhandensein mithilfe von *Agent Advertisement*-Nachrichten bekannt. Optional kann ein mobiler Knoten eine Agent Advertisement-Nachricht anfordern. Der mobile Knoten kann jeden Mobility-Agent verwenden, der über eine *Agent Solicitation*-Nachricht lokal angeschlossen ist. Ein mobiler Knoten verwendet die Agent Advertisement-Nachrichten, um festzustellen, ob sich der mobile Knoten in einem Home-Netzwerk oder in einem Foreign-Netzwerk befindet.

Der mobile Knoten verwendet einen speziellen Registrierungsprozess, um den Home-Agent über seinen aktuellen Standort zu informieren. Der mobile Knoten „überwacht" ständig, ob Mobility Agents ihr Vorhandensein bekannt geben. Diese Advertisement-Nachrichten verwendet der mobile Knoten, um festzustellen, ob er sich in ein anderes Teilnetz bewegt hat. Stellt der mobile Knoten fest, dass er seinen Standort geändert hat, verwendet er den neuen Foreign-Agent, um eine Registrierungsnachricht an den Home-Agent zu senden. Den gleichen Prozess verwendet der mobile Knoten, wenn er sich von einem Foreign-Netzwerk in ein anderes Foreign-Netzwerk bewegt.

Erkennt der mobile Knoten, dass er sich im Home-Netzwerk befindet, verwendet er die Mobility-Services nicht länger. Kehrt der mobile Knoten in sein Home-Netzwerk zurück, *hebt er die Registrierung* beim Home-Agent auf.

Agent-Erkennung

Ein mobiler Knoten verwendet eine Methode mit der Bezeichnung *Agent-Erkennung* (Agent Discoverty), um Folgendes festzustellen:

- Ob sich der Knoten von einem Netzwerk in ein anderes bewegt hat
- Ob es sich bei dem Netzwerk um das Home-Netzwerk oder um ein Foreign-Netzwerk handelt
- Die Care-Of-Adresse des Foreign-Agent, die von jedem Foreign-Agent in diesem Netzwerk angeboten wird
- Mobility-Services, die vom Mobility-Agent bereitgestellt werden. Sie werden als Flags und zusätzliche Erweiterungen in den Agent Advertisement-Nachrichten bekannt gegeben.

Mobility-Agents senden *Agent Advertisement-Nachrichten*, um ihre Services in einem Netzwerk bekannt zu geben. Wenn keine Agent Advertisement-Nachrichten vorhanden sind, kann ein mobiler Knoten Advertisement-Nachrichten auch anfordern. Diese Fähigkeit wird als *Agent Solicitation* bezeichnet. Wenn ein mobiler Knoten in der Lage ist, seine eigene co-located Care-Of-Adresse zu unterstützen, kann er normale Router Advertisement-Nachrichten für die gleichen Zwecke verwenden.

Agent Advertisement

Mobile Knoten verwenden Agent Advertisement-Nachrichten, um den aktuellen Anschlusspunkt zum Internet oder dem Netzwerk einer Organisation zu ermitteln. Eine Agent Advertisement-Nachricht ist eine Internet Control Message Protocol (ICMP) Router-Advertisement, die erweitert wurde, so dass sie die Erweitung einer Mobility Agent Advertisement aufnehmen kann.

Ein Foreign-Agent (FA) ist eventuell zu beschäftigt, um weitere mobile Knoten zu bedienen. Dennoch muss ein Foreign-Agent weiterhin Agent Advertisement-Nachrichten senden. An diesen Nachrichten erkennt ein mobile Knoten, der bereits beim Foreign-Agent registriert ist, dass er sich nicht aus dem Bereich des Foreign-Agent bewegt hat. Außerdem erkennt der mobile Knoten, dass der Foreign-Agent nicht ausgefallen ist. Ein mobiler Knoten, der bei einem Foreign-Agent registriert ist, von dem er keine Agent Advertisement-Nachrichten mehr erhält, erkennt wahrscheinlich, dass diesen Foreign-Agent nicht mehr kontaktieren kann.

Agent Advertisement-Nachrichten über dynamische Schnittstellen

Sie können die Implementierung eines Foreign-Agent so konfigurieren, dass die Agent Advertisement-Nachrichten über dynamisch erstellte Schnittstellen gesendet werden. Dazu stehen Ihnen Optionen zur Verfügung, mit denen Sie eingeschränkte, unaufgeforderte Advertisement-Nachrichten über die bekannt gebenden Schnittstellen aktivieren oder deaktivieren können. Dynamisch erstellte Schnittstellen sind Schnittstellen, die nach dem Start des `mipagent`-Daemons konfiguriert werden. Eine Advertisement-Nachricht über dynamische Schnittstellen eignet sich insbesondere für Anwendungen, die nichtstationäre Mobility-Schnittstellen unterstützen. Darüber hinaus wird durch das Einschränken von unaufgeforderten Advertisement-Nachrichten Netzwerkbandbreite eingespart.

Agent Solicitation

Jeder mobile Knoten sollte die Agent Solicitation unterstützen. Mobile Knoten verwenden die gleichen Verfahren, Standardeinstellungen und Konstanten für die Agent Solicitation, die für die Solicitation-Nachrichten von ICMP-Routern vorgegeben sind.

Die Häufigkeit, mit der ein mobiler Knoten Solicitation-Nachrichten sendet, wird durch den mobilen Knoten begeschränkt. Der mobile Knoten kann drei erste Solicitation-Nachrichten mit einer maximalen Häufigkeit von einer Nachricht pro Sekunde senden, während er nach einem Agenten sucht. Nachdem der mobile Knoten bei einem Agenten registriert ist, wird die Häufigkeit der Solicitation-Nachrichten reduziert, um den Overhead im lokalen Netzwerk zu beschränken.

Care-of-Adressen

Mobile IP bietet die folgenden alternativen Modi zum Beziehen einer Care-Of-Adresse:

- Ein Foreign-Agent stellt eine *Foreign-Agent Care-Of-Adresse* bereit, die dem mobilen Knoten über Agent Advertisement-Nachrichten bekannt gegeben wird. Die Care-Of-Adresse ist in der Regel die IP-Adresse des Foreign-Agent, der die Advertisement-Nachrichten sendet. Der Foreign-Agent ist der Tunnelendpunkt. Nachdem ein Foreign-Agent Datagramme durch einen Tunnel empfangen hat, entkapselt er die Datagramme und stellt die inneren Datagramme an den mobilen Knoten zu. Entsprechend können mehrere mobile Knoten die gleiche Care-Of-Adresse gemeinsam verwenden. Bandbreite ist bei drahtlosen Verbindungen von großer Wichtigkeit. Drahtlose Verbindungen bieten sich an, wenn Foreign-Agents Mobile IP-Services verdrahteter Verbindungen mit höherer Bandbreite anbieten.
- Ein mobiler Knoten bezieht eine *co-located Care-Of-Adresse* als über bestimmte externe Abläufe eine lokale IP-Adresse. Der mobile Knoten wird dann einer der eigenen Netzwerkschnittstellen zugeordnet. Er kann die Adresse über DHCP als temporäre Adresse beziehen. Die Adresse kann als langfristige Adresse auch das Eigentum des mobilen

Knotens werden. In jedem Fall kann der mobile Knoten die Adresse nur so lange verwenden, wie sein Besuch in dem Teilnetz andauert, zu dem die Care-Of-Adresse gehört. Wenn eine co-located Care-Of-Adresse verwendet wird, arbeitet der mobile Knoten als Endpunkt des Tunnels. Der mobile Knoten führt die Entkapselung der Datagramme durch, die ihm durch einen Tunnel zugestellt wurden.

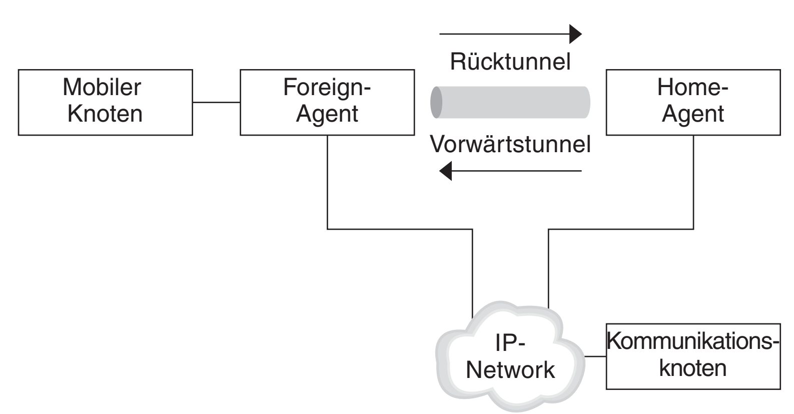
Mit einer co-located Care-Of-Adresse kann ein mobiler Knoten auch ohne einen Foreign-Agent arbeiten. Entsprechend kann ein mobiler Knoten eine co-located Care-Of-Adresse in Netzwerken verwenden, in denen kein Foreign-Agent bereitgestellt wurde.

Verwendet ein mobiler Knoten eine co-located Care-Of-Adresse, muss er sich auf dem Link befinden, der durch das Netzwerkpräfix der Care-Of-Adresse gekennzeichnet ist. Andernfalls können Datagramme mit der Care-Of-Adresse als Ziel nicht zugestellt werden.

Mobile IP mit Rücktunnel

In dem Abschnitt „Arbeitsweise von Mobile IP" auf Seite 726 wird davon ausgegangen, dass das Routing innerhalb des Internet unabhängig von der Quelladresse des Datagramms erfolgt. Dennoch prüfen die zwischengeschalteten Router eventuell auf eine topologische korrekte Quelladresse. Falls ein zwischengeschalteter Router eine Prüfung solche durchführt, muss der mobile Knoten einen Rücktunnel einrichten. Durch Einrichten eines Rücktunnels von der Care-Of-Adresse zum Home-Agent stellen Sie sicher, dass eine topologische korrekte Quelladresse für das IP-Datenpaket verwendet wird. Die Unterstützung für Rücktunnel wird von Foreign-Agents und Home-Agents bekannt gegeben. Ein mobiler Knoten kann beim Registrieren einen Rücktunnel zwischen einem Foreign-Agent und dem Home-Agent anfordern. Ein Rücktunnel ist ein Tunnel, der mit der Care-Of-Adresse des mobilen Knotens beginnt und am Home-Agent endet. Die folgende Abbildung zeigt eine Mobile IP-Topologie, in der ein Rücktunnel verwendet wird.

ABBILDUNG 27–4 Mobile IP mit einem Rücktunnel

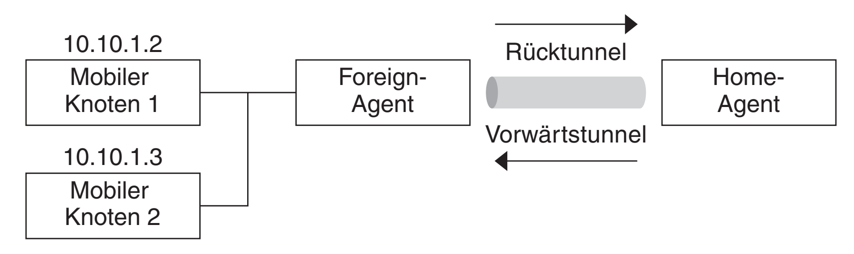


Eingeschränkte Unterstützung für private Adressen

Mobile Knoten, die über eine private Adresse verfügen, die nicht global über das Internet geroutet werden können, benötigen Rücktunnel. Solaris Mobile IP unterstützt mobile Knoten, die über eine private Adresse verfügen. Funktionen, die Solaris Mobile IP nicht unterstützt, sind unter „Overview of the Solaris Mobile IP Implementation" auf Seite 759 aufgeführt.

Unternehmen verwenden private Adressen, wenn keine externe Konnektivität erforderlich ist. Private Adressen können nicht über das Internet geroutet werden. Verfügt ein mobiler Knoten über eine private Adresse, kann er nur mit einem Kommunikatinsknoten kommunizieren, indem seine Datagramme in einem Rücktunnel an den Home-Agent gesendet werden. Der Home-Agent leitet das Datagramm dann so an den Kommunikationsknoten weiter, als ob sich der mobile Knoten im Home-Netzwerk befände. In der folgenden Abbildung ist eine Netzwerktopologie mit zwei mobilen Knoten dargestellt, die über private Adressen verfügen. Die beiden mobilen Knoten verwenden die gleiche Care-Of-Adresse, wenn sie beim gleichen Foreign-Agent registriert sind.

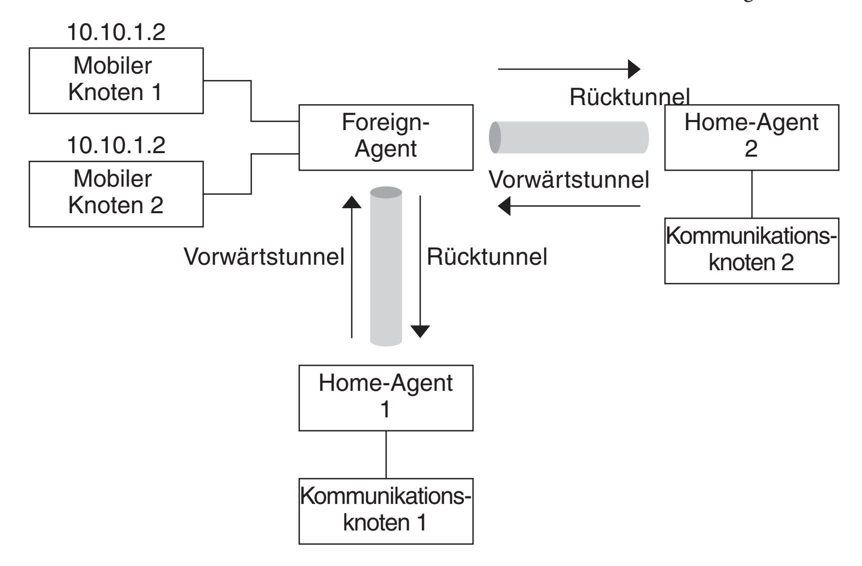
ABBILDUNG 27–5 Mobile Knoten mit privaten Adressen im gleichen Foreign-Netzwerk



Bei der Care-Of-Adresse und der Home-Agent-Adresse muss es sich um global routfähige Adressen handeln, wenn diese Adressen zu unterschiedlichen Domänen gehören, die über das öffentliche Internet miteinander verbunden sind.

Das gleiche Foreign-Netzwerk kann zwei mobile Knoten enthalten, die mit der gleichen IP-Adresse privat adressiert werden können. Jedoch müssen die beiden mobilen Knoten über unterschiedliche Home-Agents verfügen. Darüber hinaus muss sich jeder mobile Knoten in einem anderen bekannt gebenden Teilnetz eines Foreign-Agent befinden. In der folgenden Abbildung ist eine Netzwerktopologie dargestellt, die diese Situation widerspiegelt.

ABBILDUNG 27–6 Privat adressierte mobile Knoten in unterschiedlichen Foreign-Netzwerken



Mobile IP-Registrierung

Mobile Knoten können an den Agent Advertisement-Nachrichten erkennen, ob sie von einem Teilnetz zu einem anderen Teilnetz bewegt wurden. Wenn ein mobiler Knoten eine Agent Advertisement-Nachricht empfängt, die darauf hindeutet, dass er den Standort gewechselt hat, registriert er sich über einen Foreign-Agent. Auch wenn der mobile Knoten seine eigene co-located Care-Of-Adresse bezogen hat, ist es Standorten über diese Funktion möglich, den Zugriff auf Mobility-Services einzuschränken.

Die Mobile IP-Registrierung stellt einen flexiblen Mechanismus für mobile Knoten dar, die aktuellen Daten zur Erreichbarkeit an den Home-Agent zu übermitteln. Mit dem Registrierungsprozess können mobile Knoten die folgenden Aufgaben durchführen:

- Anforderungen von Weiterleitungsdiensten beim Besuch eines Foreign-Netzwerk
- Informieren des Home-Agent über die aktuelle Care-Of-Adresse

- Erneuern einer ablaufenden Registrierung
- Aufheben der Registrierung, wenn der mobile Knoten ins Home-Netzwerk zurückkehrt
- Anfordern eines Rücktunnels

Registrierungsnachrichten tauschen Informationen zwischen einem mobilen Knoten, einem Foreign-Agent und einem Home-Agent aus. Durch eine Registrierung wird eine Mobility-Bindung zum Home-Agent erstellt oder geändert. Außerdem wird durch eine Registrierung die Home-Adresse des mobilen Knotens für die angegebene Lebensdauer mit der Care-Of-Adresse des mobilen Knotens verknüpft.

Darüber hinaus ermöglicht der Registrierungsprozess mobilen Knoten das Durchführen folgender Funktionen:

- Registrieren bei mehreren Foreign-Agents
- Aufheben der Registrierung bestimmter Care-Of-Adressen, während andere Mobility-Bindungen beibehalten werden
- Erfassen der Adresse eines Home-Agent, wenn der mobile Knoten nicht mit diesen Informationen konfiguriert wurde

Mobile IP definiert die folgenden Registrierungsprozesse für einen mobilen Knoten:

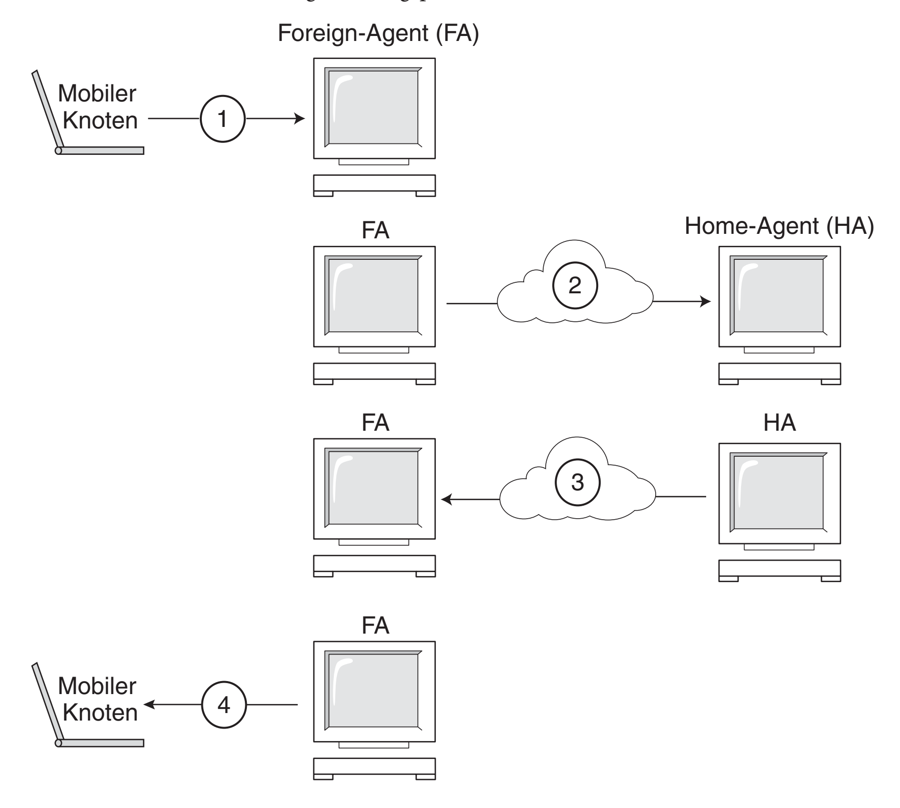
- Wenn ein mobiler Knoten eine Foreign-Agent Care-Of-Adresse registriert, informiert er den Home-Agent, dass er über diesen Foreign-Agent erreichbar ist.
- Wenn ein mobiler Knoten eine Agent Advertisement-Nachricht empfängt, die eine Registrierung über einen Foreign-Agent erfordert, kann er weiterhin versuchen, eine co-located Care-Of-Adresse zu beziehen. Der mobile Knoten kann sich auch bei diesem Foreign-Agent oder einem anderen Foreign-Agent auf diesem Link registrieren.
- Wenn der mobile Knoten eine co-located Care-Of-Adresse verwendet, kann er sich direkt beim Home-Agent registrieren.
- Wenn der mobile Knoten in sein Home-Netzwerk zurückkehrt, hebt er die Registrierung bei dem Home-Agent auf.

Diese Registrierungsprozesse beinhalten den Austausch von Registrierungsanforderungen und zugehörigen Antwortnachrichten. Wenn ein mobiler Knoten mithilfe eines Foreign-Agent registriert wird, setzt sich der Registrierungsprozess aus den folgenden Schritten zusammen, die auch in der nachstehenden Abbildung gezeigt werden:

1. Zum Einleiten des Registrierungsprozesses sendet der mobile Knoten eine Registrierungsanforderung an den künftigen Foreign-Agent.
2. Der Foreign-Agent verarbeitet die Registrierungsanforderung und leitet sie an den Home-Agent weiter.
3. Der Home-Agent sendet eine Registrierungsantwort an den Foreign-Agent, in der die Anforderung gewährt oder verweigert wird.

4. Der Foreign-Agent verarbeitet die Registrierungsantwort und leitet sie an den mobilen Knoten weiter, um ihn über den Status der Anforderung zu informieren.

ABBILDUNG 27–7 Mobile IP-Registrierungsprozess



Wenn sich der mobile Knoten direkt beim Home-Agent registriert, umfasst der Registrierungsprozess nur die folgenden Schritte:

- Der mobile Knoten sendet eine Registrierungsanforderung an den Home-Agent.
- Der Home-Agent sendet eine Registrierungsantwort an den mobilen Knoten, in der die Anforderung gewährt oder verweigert wird.

Darüber hinaus könnte der Foreign-Agent oder der Home-Agent einen Rücktunnel erfordern. Wenn der Foreign-Agent einen Rücktunnel unterstützt, verwendet der mobile Knoten den Registrierungsprozess, um einen Rücktunnel anzufordern. Der mobile Knoten setzt das Rücktunnel-Flag in der Registrierungsanforderung, um einen Rücktunnel anzufordern.

Network Access Identifier (NAI)

Authentifizierung, Autorisierung und Accounting (AAA)-Server im Internet stellen Authentifizierungs- und Autorisierungsservices für DFÜ-Computer zur Verfügung. Diese Services sind auch für mobile Knoten, die Mobile IP verwenden, wertvoll, wenn die Knoten versuchen, eine Verbindung mit fremden Domänen mit AAA-Servern herzustellen. AAA-Server verwenden die Network Access Identifier (NAI), um Clients zu identifizieren. Ein mobiler Knoten kann sich selbst identifizieren, indem der NAI mit in die Mobile IP-Registrierungsanforderung aufgenommen wird.

Da der NAI im Allgemeinen dazu verwendet wird, einen mobilen Knoten eindeutig zu identifizieren, ist die Home-Adresse des mobilen Knotens nicht immer für diese Funktion erforderlich. Somit kann sich ein mobiler Knoten selbst authentifizieren. Entsprechend kann ein mobiler Knoten auch dann zum Herstellen einer Verbindung mit der fremden Domäne autorisiert werden, wenn er keine Home-Adresse aufweisen kann. Um die Zuweisung einer Home-Adresse anzufordern, kann eine Nachricht, die die NAI-Erweiterung des mobilen Knotens enthält, das Feld für die Home-Adresse in der Registrierungsaufforderung auf null setzen.

Mobile IP-Nachrichtenauthentifizierung

Jeder mobile Knoten, Foreign-Agent und Home-Agent unterstützt eine Mobility-Sicherheitszuordnung zwischen den verschiedenen Mobile IP-Komponenten. Die Sicherheitszuordnung wird vom Security Parameter Index (SPI) und der IP-Adresse mit einem Index versehen. Bei einem mobilen Knoten ist diese Adresse die Home-Adresse des mobilen Knotens. Registrierungsnachrichten zwischen einem mobilen Knoten und dem Home-Agent werden anhand der Mobile-Home-Authentifizierungserweiterung in ihrer Echtheit bestätigt. Neben der obligatorischen Mobile-Home-Authentifizierung können Sie die optionalen Mobile-Foreign-Agent- und Home-Foreign-Agent-Authentifizierungen verwenden.

Registrierungsanforderung eines mobilen Knotens

Ein mobiler Knoten verwendet eine *Registrierungsanforderung*-Nachricht, um sich bei dem Home-Agent zu registrieren. Als Reaktion kann der Home-Agent eine Mobility-Bindung für diesen mobilen Knoten erstellen oder ändern (beispielsweise mit einer neuen Lebensdauer). Der Foreign-Agent kann die Registrierungsanforderung an den Home-Agent weiterleiten. Will der mobile Knoten jedoch eine co-located Care-Of-Adresse registrieren, kann der mobile Knoten die Registrierungsanforderung direkt an den Home-Agent senden. Wenn der Foreign-Agent bekannt gibt, das Registrierungsnachrichten an den Foreign-Agent gesendet werden müssen, muss der mobile Knoten die Registrierungsanforderung an den Foreign-Agent senden.

Antwort auf eine Registrierungsanforderung

Ein Mobility-Agent gibt eine *Registrierungsantwort*-Nachricht an einen mobilen Knoten zurück, der eine Registrierungsanforderung gesendet hat. Hat der mobile Knoten einen Service von Foreign-Agent angefordert, empfängt dieser Foreign-Agent die Antwort vom Home-Agent. Entsprechend leitet der Foreign-Agent die Antwort an den mobilen Knoten weiter. Die Antwort enthält die erforderlichen Codes, um den mobilen Knoten und den Foreign-Agent über den Status der Registrierungsanforderung zu informieren. Darüber hinaus enthält die Nachricht die, die vom Home-Agent gewährte Lebensdauer. Die Lebensdauer kann geringer als in der ursprünglichen Anforderung ausfallen. Außerdem kann eine Registrierungsanforderung eine dynamisch zugewiesene Home-Adresse enthalten.

Überlegungen zum Foreign-Agent

Der Foreign-Agent spielt bei der Mobile IP-Registrierung im Wesentlichen eine passive Rolle. Der Foreign-Agent fügt alle registrierten mobilen Knoten einer Besuchertabelle hinzu. Außerdem leitet er Registrierungsanforderungen und -antworten zwischen den mobilen Knoten und Home-Agent weiter. Wenn der Foreign-Agent die Care-Of-Adresse bereitstellt, führt er darüber hinaus die Entkapselung von Datagrammen durch, so dass der Inhalt an die mobilen Knoten zugestellt werden kann. Weiterhin sendet der Foreign-Agent in regelmäßigen Abständen Agent Advertisement-Nachrichten, um sein Vorhandensein bekannt zu geben.

Wenn Home-Agents und Foreign-Agents Rücktunnel unterstützen und der mobile Knoten einen Rücktunnel anfordert, sendet der Foreign-Agent alle Pakete vom mobilen Knoten durch einen Tunnel an den Home-Agent. Der Home-Agent sendet die Pakete an den Kommunikationsknoten. Dieser Prozess ist die Umkehr des Home-Agent-Tunneling aller Pakete des mobilen Knoten an den Foreign-Agent zur Zustellung an den mobilen Knoten. Ein Foreign-Agent, der einen Rücktunnel unterstützt, meldet, dass ein Rücktunnel bei der Registrierung unterstützt wird. Aufgrund der lokalen Richtlinie kann der Foreign-Agent eine Registrierungsanforderung verweigern, wenn das Rücktunnel-Flag nicht gesetzt ist. Der Foreign-Agent kann mehrere mobile Knoten mit der gleichen (privaten) IP-Adresse nur dann unterscheiden, wenn die mobilen Knoten unterschiedliche Schnittstellen des Foreign-Agent besuchen. Bei einem Vorwärtstunnel unterscheidet der Foreign-Agent mehrere mobile Knoten, die die gleiche private Adresse nutzen, in dem er die eingehende Tunnelschnittstelle prüft. Die eingehende Tunnelschnittstelle ist einer einmaligen Home-Agent-Adresse zugeordnet.

Überlegungen zum Home-Agent

Home-Agents spielen eine aktive Rolle im Registrierungsprozess. Der Home-Agent empfängt die Registrierungsanforderungen vom mobilen Knoten. Die Registrierungsanforderung könnte von dem Foreign-Agent weitergeleitet worden sein. Der Home-Agent aktualisiert seine Aufzeichnungen zu den Mobility-Bindungen dieses mobilen Knotens. Der Home-Agent erteilt

auf jede Registrierungsanforderung eine geeignete Registrierungsantwort. Darüber hinaus leitet der Home-Agent Datenpakete an den mobilen Knoten weiter, wenn sich dieser nicht im Home-Netzwerk befindet.

Ein Home-Agent hat eventuell kein physikalisches Teilnetz für mobile Knoten konfiguriert. Dennoch muss der Home-Agent die Home-Adresse des mobilen Knotens über die Datei `mipagent.conf` oder einen anderen Mechanismus erkennen, wenn er die Registrierung genehmigt. Weitere Informationen zur Datei `mipagent.conf` finden Sie unter „Erstellen einer Mobile IP-Konfigurationsdatei“ auf Seite 744.

Ein Home-Agent kann privat adressierte mobile Knoten unterstützen, indem er die privat adressierten mobilen Knoten in der Datei `mipagent.conf` konfiguriert. Die von dem Home-Agent verwendeten Home-Adressen müssen einmalig sein.

Dynamische Home-Agent-Erkennung

In bestimmten Situationen kennt der mobile Knoten die Adresse seines Home-Agents nicht, wenn er sich zu registrieren versucht. In diesem Fall kann er eine dynamische Home-Agent-Adressauflösung verwenden, um die Adresse in Erfahrung zu bringen. Dazu setzt er das Home-Agent-Feld in der Registrierungsaufforderung auf die Teilnetz-gesteuerte Broadcast-Adresse seines Home-Netzwerk. Jeder Home-Agent, der eine Registrierungsaufforderung mit einer Broadcast-Zieladresse empfängt, lehnt die Registrierung des mobilen Knotens ab, in dem eine entsprechende Antwortnachricht gesendet wird. Jetzt kann der mobile Host beim nächsten Registrierungsversuch die Unicast-IP-Adresse des Home-Agent verwenden, die in der negativen Antwortnachricht angegeben ist.

Routen von Datagrammen von und an mobile Knoten

In diesem Abschnitt wird beschrieben, wie mobile Knoten, Home-Agents und Foreign-Agents zusammenarbeiten, um Datagramme für mobile Knoten, die an ein Foreign-Netzwerk angeschlossen sind, zu routen. Informationen zu den von Solaris OS unterstützten Mobile IP-Funktionen finden Sie unter „Overview of the Solaris Mobile IP Implementation“ auf Seite 759.

Methoden zur Einkapselung

Home-Agents und Foreign-Agents nutzen eine der verfügbaren Einkapselungsmethoden, um Datagramme zu unterstützen, die einen Tunnel verwenden. Definierte Einkapselungsmethoden sind IP-in-IP Encapsulation, Minimal Encapsulation und Generic Routing Encapsulation. Foreign-Agent und Home-Agent-Fälle oder indirekt co-located mobile Knoten und Home-Agent-Fälle müssen die gleiche Einkapselungsmethode unterstützen. Alle Mobile IP-Einheiten müssen die IP-in-IP Encapsulation unterstützen.

Routing von Unicast Datagrammen

Wenn ein mobiler Knoten in einem Foreign-Netzwerk registriert ist, verwendet er die folgenden Regeln, um einen Standard-Router zu wählen:

- Ist der mobile Knoten registriert, und verwendet er eine Agent Care-Of-Adresse, ist der Prozess recht einfach. Der mobile Knoten wählt seinen Standard-Router unter den Router-Adressen, die im ICMP-Router-Advertisement-Teil der Agent Advertisement-Nachrichten bekannt gegeben werden. Alternativ kann der mobile Knoten die IP-Quelladresse der Agent Advertisement-Nachricht als mögliche Option für die IP-Adresse eines Standard-Routers wählen.
- Der mobile Knoten kann unter Verwendung einer co-located Care-Of-Adresse direkt beim Home-Agent registriert sein. In diesem Fall wählt der mobile Knoten seinen Standard-Router unter den Routern, die in einer der empfangenen ICMP-Router Advertisement-Nachrichten bekannt gegeben werden. Das Netzwerkpräfix des ausgewählten Standard-Routers muss mit dem Netzwerkpräfix der extern bezogenen Care-Of-Adresse des mobilen Knotens übereinstimmen. Die Adresse kann mit der IP-Quelladresse der Agent Advertisement-Nachricht unter dem Netzwerkpräfix identisch sein. In diesem Fall kann der mobile Knoten diese IP-Quelladresse als andere mögliche Option für eine IP-Adresse eines Standard-Routers wählen.
- Ist der mobile Knoten registriert, leitet ein Foreign-Agent, der einen Rücktunnel unterstützt, Unicast-Datagramme vom mobilen Knoten durch den Rücktunnel an den Home-Agent. Ist der mobile Knoten bei einem Foreign-Agent registriert, der Rücktunnel unterstützt, muss der mobile Knoten diesen Foreign-Agent als Standard-Router verwenden.

Broadcast-Datagramme

Wenn ein Home-Agent ein Broadcast- oder Multicast-Datagramm empfängt, leitet er das Datagramm nur an mobile Knoten weiter, die den Empfang dieser Datagramme explizit angefordert haben. Wie der Home-Agent Broadcast- und Multicast-Datagramme an mobile Knoten weiterleitet, hängt im Wesentlichen von zwei Faktoren ab: entweder verwendet der mobile Knoten eine von einem Foreign-Agent bereitgestellte Care-Of-Adresse, oder der mobile Knoten verwendet seine eigene co-located Care-Of-Adresse. Bei der erstgenannten Option muss das Datagramm doppelt gekapselt werden. Der erste IP-Header identifiziert den mobilen Knoten, an den das Datagramm zugestellt werden soll. Der erste IP-Header ist nicht im Broadcast- oder Multicast-Datagramm enthalten. Der zweite IP-Header identifiziert die Care-Of-Adresse und ist der normale Tunnel-Header. Im zweiten Szenario entkapselt der mobile Knoten seine eigenen Datagramme, und die Datagramme müssen über den regulären Tunnel gesendet werden.

Routing von Multicast-Datagrammen

Um den Empfang von Multicast-Verkehr zu beginnen, wenn ein mobiler Knoten ein fremdes Teilnetz besucht, kann ein mobiler Knoten unter Verwendung einer der folgenden Methoden einer Multicast-Gruppe beitreten:

- Nutzt der mobile Knoten eine co-located Care-Of-Adresse, kann er diese Adresse als IP-Quelladresse in einer Internet Group Management Protocol (IGMP)-Beitrittsnachricht verwenden. In diesem Fall muss jedoch ein Multicast-Router im besuchten Teilnetz vorhanden sein.
- Möchte der mobile Knoten der ICMP-Gruppe in seinem Home-Teilnetz beitreten, muss er einen Rücktunnel verwenden, um IGMP-Beitrittsnachrichten an den Home-Agent zu senden. In diesem Fall muss der Home-Agent des mobilen Knotens ein Multicast-Router sein. Der Home-Agent kann dann Multicast-Datagramme durch den Tunnel an den mobilen Knoten weiterleiten.
- Nutzt der mobile Knoten eine co-located Care-Of-Adresse, kann er diese Adresse als IP-Quelladresse in einer IGMP-Beitrittsnachricht verwenden. In diesem Fall muss jedoch ein Multicast-Router im besuchten Teilnetz vorhanden sein. Nachdem der mobile Knoten einer Gruppe beigetreten ist, kann er am Netzverkehr teilnehmen, indem er seine eigenen Multicast-Pakete direkt in das besuchte Netzwerk sendet.
- Direkt im besuchten Netzwerk senden.
- Durch einen Tunnel an den Home-Agent senden.

Multicast-Routing hängt von der IP-Quelladresse ab. Ein mobiler Knoten, der ein Multicast-Datagramm sendet, muss das Datagramm von einer gültigen Quelladresse auf diesem Link senden. Daher muss ein mobiler Knoten, der Multicast-Datagramme direkt in das besuchte Netzwerk sendet, eine co-located Care-Of-Adresse als IP-Quelladresse verwenden. Außerdem muss der mobile Knoten der Multicast-Gruppe beigetreten sein, der diese Adresse zugeordnet ist. Entsprechend gilt, ein mobiler Knoten, der in seinem Home-Teilnetz vor dem Roaming einer Multicast-Gruppe beigetreten ist oder der Multicast-Gruppe während des Roaming durch einen Rücktunnel zu seinem Home-Agent beigetreten ist, muss seine Home-Adresse als IP-Quelladresse des Multicast-Datagramms verwenden. Das bedeutet, der mobile Knoten muss diese Datagramme auch über den Rücktunnel an sein Home-Teilnetz senden, entweder über sich selbst (über seine co-located Care-Of-Adresse) oder über den Rücktunnel eines Foreign-Agent.

Obwohl es für einen mobilen Knoten sinnvoll erscheint, immer von dem Teilnetz aus beizutreten, das der mobile Knoten besucht, so ist er dennoch ein mobiler Knoten. Entsprechend muss der mobile Knoten jedes Mal neu beitreten, wenn er die Teilnetze wechselt. Daher ist es für den mobilen Knoten am sinnvollsten, über seinen Home-Agent beizutreten und diesen Overhead nicht zu verursachen. Darüber hinaus sind eventuell Multicast-Sitzungen vorhanden, die nur vom Home-Teilnetz aus verfügbar sind. Andere Überlegungen zwingen den mobilen Knoten eventuell dazu, in einer bestimmten Weise teilzunehmen.

Sicherheitsbetrachtungen für Mobile IP

In vielen Situationen stellen mobile Computer eine Verbindung mit dem Netzwerk drahtlos her. Drahtlose Verbindungen durch passives Mithören, aktive Replay-Angriffe und andere aktive Angriffe besonders gefährdet.

Da Mobile IP erkannt hat, dass es diese Gefährdung weder reduzieren noch eliminieren kann, verwendet es eine Art Authentifizierung, um Mobile IP-Registrierungsnachrichten vor dieser Art Angriffen zu schützen. Der verwendete Standardalgorithmus ist MD5 mit einer Schlüsselgröße von 128 Bit. Der standardmäßige Betriebsmodus erfordert, dass dieser 128-Bit-Schlüssel vor und hinter Daten steht, an denen ein Hash-Algorithmus angewendet wird. Der Foreign-Agent verwendet MD5, um diese Authentifizierung zu unterstützen. Darüber hinaus verwendet der Foreign-Agent Schlüssel von 128 Bit oder größer mit einer manuellen Schlüsselverteilung. Mobile IP kann weitere Authentifizierungsalgorithmen, Algorithmus-Modi, Schlüsselverteilungsmethoden und Schlüsselgrößen unterstützen.

Diese Methoden verhindern, dass Mobile IP-Registrierungsnachrichten geändert werden. Jedoch verwendet Mobile IP auch eine Form von Replay-Schutz, um Mobile IP-Einheiten zu warnen, wenn sie Duplikate von früheren Mobile IP-Registrierungsnachrichten empfangen. Wenn diese Schutzmethoden nicht verwendet werden, sind der mobile Knoten und sein Home-Agent eventuell nicht mehr synchron, wenn einer von ihnen eine Registrierungsnachricht empfängt. Aus diesem Grund aktualisiert Mobile IP seinen Status. Angenommen, ein Home-Agent empfängt eine doppelte Nachricht zum Aufheben einer Registrierung, während der mobile Knoten über einen Foreign-Agent registriert ist.

Der Replay-Schutz wird über eine Methode sichergestellt, die als *nonces* oder *timestamps* bezeichnet wird. Nonces und timestamps werden zwischen Home-Agents und mobilen Knoten mit den Mobile IP-Registrierungsnachrichten ausgetauscht. Nonces und timestamps sind durch einen Authentifizierungsmechanismus vor Änderungen geschützt. Entsprechend kann, wenn ein Home-Agent oder ein mobiler Knoten eine doppelt vorhandenen Nachricht empfängt, das Duplikat gelöscht werden.

Bei der Verwendung von Tunneln besteht eine besondere Gefährdung, insbesondere dann, wenn die Registrierung nicht authentifiziert werden kann. So ist das Address Resolution Protocol (ARP) nicht authentifiziert und kann potentiell verwendet werden, um den Datenverkehr anderer Hosts zu „stehlen".

KAPITEL 28

Verwalten von Mobile IP (Aufgaben)

In diesem Kapitel werden Verfahren zum Ändern, Hinzufügen, Löschen und Anzeigen von Parametern in der Mobile IP-Konfigurationsdatei beschrieben. Darüber hinaus finden Sie hier Informationen zum Anzeigen des Status eines Mobility-Agent.

Dieses Kapitel enthält die folgenden Informationen:

- „Erstellen einer Mobile IP-Konfigurationsdatei (Übersicht der Schritte)" auf Seite 743
- „Erstellen einer Mobile IP-Konfigurationsdatei" auf Seite 744
- „Ändern einer Mobile IP-Konfigurationsdatei" auf Seite 749
- „Ändern der Mobile IP-Konfigurationsdatei (Übersicht der Schritte)" auf Seite 748
- „Anzeigen des Mobility-Agent-Status" auf Seite 756
- „Anzeigen der Mobility-Routen auf einem Foreign-Agent" auf Seite 757

Eine Einführung in Mobile IP finden Sie in Kapitel 27, „Mobile IP (Übersicht)". Ausführliche Informationen zu Mobile IP finden Sie in Kapitel 29, „Mobile IP-Dateien und Befehle (Referenz)".

Hinweis – Die Mobile IP-Funktion ist in Solaris 10-Aktualisierungen nach Solaris 10 8/07 nicht mehr vorhanden.

Erstellen einer Mobile IP-Konfigurationsdatei (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Erstellen einer Mobile IP-Konfigurationsdatei.	Erstellen Sie eine Datei `/etc/inet/mipagent.conf` oder Kopieren Sie eine der Beispieldateien.	„So erstellen Sie eine Mobile IP-Konfigurationsdatei" auf Seite 745

Aufgabe	Beschreibung	Siehe
Konfigurieren des Abschnitts `General`.	Geben Sie die Versionsnummer in den Abschnitt `General` der Mobile IP-Konfigurationsdatei ein.	„So konfigurieren Sie den Abschnitt `General`“ auf Seite 746
Konfigurieren des Abschnitts `Advertisements`.	Fügen Sie Label und Werte hinzu bzw. ändern Sie diese Angaben im Abschnitt `Advertisements` der Mobile IP-Konfigurationsdatei.	„So konfigurieren Sie den Abschnitt `Advertisements`“ auf Seite 746
Konfigurieren des Abschnitts `GlobalSecurityParameters`.	Fügen Sie Label und Werte hinzu bzw. ändern Sie diese Angaben im Abschnitt `GlobalSecurityParameters` der Mobile IP-Konfigurationsdatei.	„So konfigurieren Sie den Abschnitt `GlobalSecurityParameters`“ auf Seite 746
Konfigurieren des Abschnitts `Pool`.	Fügen Sie Label und Werte hinzu bzw. ändern Sie diese Angaben im Abschnitt `Pool` der Mobile IP-Konfigurationsdatei.	„So konfigurieren Sie den Abschnitt `Pool`“ auf Seite 747
Konfigurieren des Abschnitts `SPI`.	Fügen Sie Label und Werte hinzu bzw. ändern Sie diese Angaben im Abschnitt `SPI` der Mobile IP-Konfigurationsdatei.	„So konfigurieren Sie den Abschnitt `SPI`“ auf Seite 747
Konfigurieren des Abschnitts `Address`.	Fügen Sie Label und Werte hinzu bzw. ändern Sie diese Angaben im Abschnitt `Address` der Mobile IP-Konfigurationsdatei.	„So konfigurieren Sie den Abschnitt `Address`“ auf Seite 747

Erstellen einer Mobile IP-Konfigurationsdatei

In diesem Abschnitt finden in Sie Informationen zur Planung von Mobile IP und zum Erstellen der `/etc/inet/mipagent.conf`-Datei.

▼ So planen Sie für Mobile IP

Wenn Sie die Datei `mipagent.conf` das erste Mal konfigurieren, müssen Sie die folgenden Aufgaben durchführen:

1 Legen Sie die Leistungsmerkmale Ihres Mobile IP-Agent fest. Dabei richten Sie nach nach den Leistungsanforderungen Ihrer Organisation:

- Nur Foreign-Agent-Funktionen
- Nur Home-Agent-Funktionen
- Sowohl Foreign-Agent- als auch Home-Agent-Funktionen

2 **Erstellen Sie die Datei** `/etc/inet/mipagent.conf`**, und geben Sie die erforderlichen Einstellungen an, indem Sie die in diesem Abschnitt beschriebenen Verfahren einsetzen. Sie können auch eine der folgenden Dateien nach** `/etc/inet/mipagent.conf` **kopieren und gemäß Ihren Anforderungen modifizieren:**

- Für Foreign-Agent-Funktionen kopieren Sie die Datei `/etc/inet/mipagent.conf.fa-sample`.
- Für Home-Agent-Funktionen kopieren Sie die Datei `/etc/inet/mipagent.conf.ha-sample`.
- Für sowohl Foreign-Agent- als auch Home-Agent-Funktionen kopieren Sie die Datei `/etc/inet/mipagent.conf-sample`.

3 **Sie können Ihr System neu starten, um das Startskript aufzurufen, mit dem der** `mipagent`**-Daemon neu gestartet wird. Alternativ können Sie den Daemon** `mipagent` **mithilfe des folgenden Befehls neu starten:**

```
# /etc/inet.d/mipagent start
```

▼ So erstellen Sie eine Mobile IP-Konfigurationsdatei

1 **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.**

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 **Erstellen Sie die Datei** `/etc/inet/mipagent.conf` **mithilfe einer der folgenden Optionen:**

- Erstellen Sie in dem Verzeichnis `/etc/inet` eine leere Datei mit der Bezeichnung `mipagent.conf`.
- Kopieren Sie eine der folgenden Beispieldateien, die Ihnen die gewünschten Leistungsmerkmale zur Verfügung stellt, in die Datei `/etc/inet/mipagent.conf`.
  - `/etc/inet/mipagent.conf.fa-sample`
  - `/etc/inet/mipagent.conf.ha-sample`
  - `/etc/inet/mipagent.conf-sample`

3 **Fügen Sie die erforderlichen Konfigurationsparameter in die Datei** `/etc/inet/mipagent.conf` **ein bzw. ändern Sie die Parameter, bis die Datei Ihren Konfigurationsanforderungen entspricht.**

In den weiteren Verfahren in diesem Abschnitt sind die Schritte beschrieben, mit denen Sie die Abschnitte in der Datei `/etc/inet/mipagent.conf` ändern.

So konfigurieren Sie den Abschnitt `General`

Wenn Sie eine der Beispieldateien in das Verzeichnis `/etc/inet` kopiert haben, können Sie dieses Verfahren überspringen, da die Beispieldatei diesen Eintrag bereits enthält. „`General`“ auf Seite 765 enthält Beschreibungen der in diesem Abschnitt verwendeten Label und Werte.

- **Fügen Sie der Datei `/etc/inet/mipagent.conf` die folgenden Zeilen hinzu:**

```
[General]
     Version = 1.0
```

Hinweis – Die Datei `/etc/inet/mipagent.conf` muss diesen Eintrag enthalten.

So konfigurieren Sie den Abschnitt `Advertisements`

„`Advertisements`“ auf Seite 765 enthält Beschreibungen der in diesem Abschnitt verwendeten Label und Werte.

- **Fügen Sie der Datei `/etc/inet/mipagent.conf` die folgenden Zeilen mit den Werten hinzu, die für Ihre Konfiguration erforderlich sind bzw. ändern Sie die entsprechenden Zeilen ab.**

```
[Advertisements interface]
     HomeAgent = <yes/no>
     ForeignAgent = <yes/no>
     PrefixFlags = <yes/no>
     AdvertiseOnBcast = <yes/no>
     RegLifetime = n
     AdvLifetime = n
     AdvFrequency = n
     ReverseTunnel = <yes/no/FA/HA/both>
     ReverseTunnelRequired = <yes/no/FA/HA>
```

Hinweis – Sie müssen für jede Schnittstelle auf dem lokalen Host, der Mobile IP-Services bereitstellt, einen eigenen `Advertisements`-Abschnitt einfügen.

So konfigurieren Sie den Abschnitt `GlobalSecurityParameters`

„`GlobalSecurityParameters`“ auf Seite 767 enthält Beschreibungen der in diesem Abschnitt verwendeten Label und Werte.

- **Fügen Sie der Datei `/etc/inet/mipagent.conf` die folgenden Zeilen mit den Werten hinzu, die für Ihre Konfiguration erforderlich sind bzw. ändern Sie die entsprechenden Zeilen ab:**

```
[GlobalSecurityParameters]
     MaxClockSkew = n
     HA-FAauth = <yes/no>
```

```
    MN-FAauth = <yes/no>
    Challenge = <yes/no>
    KeyDistribution = files
```

So konfigurieren Sie den Abschnitt `Pool`

„`Pool`“ auf Seite 768 enthält Beschreibungen der in diesem Abschnitt verwendeten Label und Werte:

1. **Bearbeiten Sie die Datei `/etc/inet/mipagent.conf`.**

2. **Fügen Sie die folgenden Zeilen mit den Werten hinzu, die für Ihre Konfiguration erforderlich sind bzw. ändern Sie die entsprechenden Zeilen ab:**

```
[Pool pool-identifier]
    BaseAddress = IP-address
    Size = size
```

So konfigurieren Sie den Abschnitt `SPI`

„`SPI`“ auf Seite 769 enthält Beschreibungen der in diesem Abschnitt verwendeten Label und Werte.

1. **Bearbeiten Sie die Datei `/etc/inet/mipagent.conf`.**

2. **Fügen Sie die folgenden Zeilen mit den Werten hinzu, die für Ihre Konfiguration erforderlich sind bzw. ändern Sie die entsprechenden Zeilen ab:**

```
[SPI SPI-identifier]
    ReplayMethod = <none/timestamps>
    Key = key
```

Hinweis – Sie müssen für jeden bereitgestellten Sicherheitskontext einen eigenen `SPI`-Abschnitt einfügen.

So konfigurieren Sie den Abschnitt `Address`

„`Address`“ auf Seite 770 enthält Beschreibungen der in diesem Abschnitt verwendeten Label und Werte.

1. **Bearbeiten Sie die Datei `/etc/inet/mipagent.conf`.**

2. **Fügen Sie die folgenden Zeilen mit den Werten hinzu, die für Ihre Konfiguration erforderlich sind bzw. ändern Sie die entsprechenden Zeilen ab:**

- **Bei einem mobilen Knoten geben Sie Folgendes ein:**

```
[Address address]
     Type = node
     SPI = SPI-identifier
```

- **Bei einem Agent geben Sie Folgendes ein:**

```
[Address address]
     Type = agent
     SPI = SPI-identifier
```

- **Bei einem mobilen Knoten, der durch seinen NAI identifiziert wird, verwenden Sie Folgendes:**

```
[Address NAI]
     Type = Node
     SPI = SPI-identifier
     Pool = pool-identifier
```

- **Bei einem standardmäßigen mobilen Knoten geben Sie Folgendes ein:**

```
[Address Node-Default]
     Type = Node
     SPI = SPI-identifier
     Pool = pool-identifier
```

Ändern der Mobile IP-Konfigurationsdatei (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Ändern Sie den Abschnitt `General`.	Geben Sie den Befehl `mipagentconfig change` ein, um den Wert eines Labels im Abschnitt `General` der Mobile IP-Konfigurationsdatei zu ändern.	„So ändern Sie den Abschnitt `General`“ auf Seite 749
Ändern Sie den Abschnitt `Advertisements`.	Geben Sie den Befehl `mipagentconfig change` ein, um den Wert eines Label im Abschnitt `Advertisements` der Mobile IP-Konfigurationsdatei zu ändern.	„So ändern Sie den Abschnitt `Advertisements`“ auf Seite 750
Ändern Sie den Abschnitt `GlobalSecurityParameters`.	Geben Sie den Befehl `mipagentconfig change` ein, um den Wert eines Labels im Abschnitt `GlobalSecurityParameters` der Mobile IP-Konfigurationsdatei zu ändern.	„So ändern Sie den Abschnitt `GlobalSecurityParameters`“ auf Seite 751
Ändern Sie den Abschnitt `Pool`.	Geben Sie den Befehl `mipagentconfig change` ein, um den Wert eines Labels im Abschnitt `Pool` der Mobile IP-Konfigurationsdatei zu ändern.	„So ändern Sie den Abschnitt `Pool`“ auf Seite 751

Ändern Sie den Abschnitt `SPI`.	Geben Sie den Befehl `mipagentconfig change` ein, um den Wert eines Labels im Abschnitt `SPI` der Mobile IP-Konfigurationsdatei zu ändern.	„So ändern Sie den Abschnitt `SPI`" auf Seite 752
Ändern Sie den Abschnitt `Address`.	Geben Sie den Befehl `mipagentconfig change` ein, um den Wert eines Labels im Abschnitt `Address` der Mobile IP-Konfigurationsdatei zu ändern.	„So ändern Sie den Abschnitt `Address`" auf Seite 752
Hinzufügen oder Löschen von Parametern.	Geben Sie den Befehl `mipagentconfig add` oder den Befehl `delete` ein, um neue Parameter, Label und Werte hinzuzufügen oder um vorhandene aus beliebigen Abschnitten der Mobile IP-Konfigurationsdatei zu löschen.	„So fügen einer Konfigurationsdatei Parameter hinzu bzw. löschen Parameter" auf Seite 753
Anzeigen der aktuellen Einstellungen der Parameterziele.	Geben Sie den Befehl `mipagentconfig get` ein, um die aktuellen Einstellungen eines beliebigen Abschnitts in der Mobile IP-Konfigurationsdatei anzuzeigen.	„So zeigen Sie die aktuellen Parameterwerte in der Konfigurationsdatei an" auf Seite 754

Ändern einer Mobile IP-Konfigurationsdatei

In diesem Abschnitt wird beschrieben, wie Sie die Mobile IP-Konfigurationsdatei mithilfe des Befehls `mipagentconfig` ändern. Weiterhin wird in diesem Abschnitt beschrieben, wie Sie die aktuellen Einstellungen der Parameterziele anzeigen.

„Konfiguration des Mobility IP-Agent" auf Seite 773 enthält eine konzeptuelle Beschreibung der Verwendung des Befehls `mipagentconfig`. Lesen Sie auch die Manpage `mipagentconfig`(1M).

▼ So ändern Sie den Abschnitt `General`

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Geben Sie für jedes Label, das Sie im Abschnitt `General` ändern möchten, den folgenden Befehl ein.**

```
# mipagentconfig change <label> <value>
```

Beispiel 28–1 Ändern eines Parameters im Abschnitt `General`

Im folgenden Beispiel wird gezeigt, wie Sie die Versionsnummer im Abschnitt `General` der Konfigurationsdatei ändern.

```
# mipagentconfig change version 2
```

So ändern Sie den Abschnitt `Advertisements`

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Geben Sie für jedes Label, das Sie im Abschnitt `Advertisements` ändern möchten, den folgenden Befehl ein:**

   `# mipagentconfig change adv` *device-name* `<label> <value>`

   Wenn Sie die bekannt gegebene Lebensdauer des Agenten für das Gerät `hme0` auf 300 Sekunden ändern möchten, geben Sie den folgenden Befehl ein.

   ```
   # mipagentconfig change adv hme0 AdvLifetime 300
   ```

Beispiel 28–2 Ändern des Abschnitts `Advertisements`

Im folgenden Beispiel wird gezeigt, wie Sie bestimmte Parameter im Abschnitt `Advertisements` der Konfigurationsdatei ändern.

```
# mipagentconfig change adv hme0 HomeAgent yes
# mipagentconfig change adv hme0 ForeignAgent no
# mipagentconfig change adv hme0 PrefixFlags no
# mipagentconfig change adv hme0 RegLifetime 300
# mipagentconfig change adv hme0 AdvFrequency 4
# mipagentconfig change adv hme0 ReverseTunnel yes
```

▼ So ändern Sie den Abschnitt `GlobalSecurityParameters`

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Geben Sie für jedes Label, das Sie im Abschnitt `GlobalSecurityParameters` ändern möchten, den folgenden Befehl ein:

```
# mipagentconfig change <label> <value>
```

Wenn Sie die Home-Agent- und die Foreign-Agent-Authentifizierung aktivieren möchten, geben Sie den folgenden Befehl ein:

```
# mipagentconfig change HA-FAauth yes
```

Beispiel 28–3 Ändern des Abschnitts Global Security Parameters

Im folgenden Beispiel wird gezeigt, wie Sie bestimmte Parameter im Abschnitt `GlobalSecurityParameters` der Konfigurationsdatei ändern.

```
# mipagentconfig change MaxClockSkew 200
# mipagentconfig change MN-FAauth yes
# mipagentconfig change Challenge yes
# mipagentconfig change KeyDistribution files
```

▼ So ändern Sie den Abschnitt `Pool`

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Geben Sie für jedes Label, das Sie im Abschnitt `Pool` ändern möchten, den folgenden Befehl ein:

```
# mipagentconfig change Pool pool-identifier <label> <value>
```

Beispiel 28–4 Ändern des Abschnitts `Pool`

Im folgenden Beispiel werden die Befehle gezeigt, mit denen Sie die Basisadresse des Pools `10` zu `192.168.1.1` und die Größe zu `100` ändern.

```
# mipagentconfig change Pool 10 BaseAddress 192.168.1.1
# mipagentconfig change Pool 10 Size 100
```

So ändern Sie den Abschnitt `SPI`

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Geben Sie für jedes Label, das Sie im Abschnitt `SPI` ändern möchten, den folgenden Befehl ein:**

   `# mipagentconfig change SPI` *SPI-identifier* `<label> <value>`

   Wenn Sie den Schlüssel für `SPI 257` zu `5af2aee39ff0b332` ändern möchten, geben Sie den folgenden Befehl ein.

   ```
   # mipagentconfig change SPI 257 Key 5af2aee39ff0b332
   ```

Beispiel 28–5 Ändern des Abschnitts `SPI`

Im folgenden Beispiel wird gezeigt, wie das Label `ReplayMethod` im Abschnitt `SPI` der Konfigurationsdatei geändert wird.

```
# mipagentconfig change SPI 257 ReplayMethod timestamps
```

So ändern Sie den Abschnitt `Address`

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Geben Sie für jedes Label, das Sie im Abschnitt `Address` ändern möchten, den folgenden Befehl ein:

```
# mipagentconfig change addr [NAI | IPaddr | node-default] <label> <value>
```

Eine Beschreibung der drei Konfigurationsmethoden (NAI, IP-Adresse und Knoten-Standard) finden Sie unter „`Address`“ auf Seite 770.

Wenn Sie den SPI der IP-Adresse `10.1.1.1` zu `258` ändern möchten, geben Sie den folgenden Befehl ein:

```
# mipagentconfig change addr 10.1.1.1 SPI 258
```

Beispiel 28–6 Ändern des Abschnitts `Address`

Im folgenden Beispiel wird gezeigt, wie Sie bestimmte Parameter im Abschnitt `Address` der Konfigurationsdatei ändern.

```
# mipagentconfig change addr 10.1.1.1 Type agent
# mipagentconfig change addr 10.1.1.1 SPI 259
# mipagentconfig change addr mobilenode@abc.com Type node
# mipagentconfig change addr mobilenode@abc.com SPI 258
# mipagentconfig change addr mobilenode@abc.com Pool 2
# mipagentconfig change addr node-default SPI 259
# mipagentconfig change addr node-default Pool 3
# mipagentconfig change addr 10.68.30.36 Type agent
# mipagentconfig change addr 10.68.30.36 SPI 260
```

▼ So fügen einer Konfigurationsdatei Parameter hinzu bzw. löschen Parameter

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Geben Sie für jedes Label, das Sie dem ausgewählten Abschnitt hinzufügen bzw. daraus löschen möchten, den entsprechenden Befehl ein:

- Für den Abschnitt `General` verwenden Sie den folgenden Befehl:

  ```
  # mipagentconfig [add | delete] <label> <value>
  ```

- Für den Abschnitt `Advertisements` verwenden Sie den folgenden Befehl:

  ```
  # mipagentconfig [add | delete] adv device-name <label> <value>
  ```

Hinweis – Mit der folgenden Syntax können Sie eine Schnittstelle hinzufügen:

```
# mipagentconfig add adv device-name
```

In diesem Fall werden der Schnittstelle Standardwerte zugewiesen (sowohl für Foreign-Agent als auch Home-Agent).

- Für den Abschnitt `GlobalSecurityParameters` verwenden Sie den folgenden Befehl:

  ```
  # mipagentconfig [add | delete] <label> <value>
  ```
- Für den Abschnitt `Pools` verwenden Sie den folgenden Befehl:

  ```
  # mipagentconfig [add | delete] Pool pool-identifier <label> <value>
  ```
- Für den Abschnitt `SPI` verwenden Sie den folgenden Befehl:

  ```
  # mipagentconfig [add | delete] SPI SPI-identifier <label> <value>
  ```
- Für den Abschnitt `Address` verwenden Sie den folgenden Befehl:

  ```
  # mipagentconfig [add | delete] addr [NAI | IP-address | node-default] \
  <label> <value>
  ```

Hinweis – Erstellen Sie keine identischen `Advertisements`-, `Pool`-, `SPI`- und `Address`-Abschnitte.

Beispiel 28–7 Ändern der Dateiparameter

Um beispielsweise einen neuen Adresspool (Pool 11) zu erstellen, der die Basisadresse `192.167.1.1` und eine Größe von `100` besitzt, verwenden Sie die folgenden Befehle.

```
# mipagentconfig add Pool 11 BaseAddress 192.167.1.1
# mipagentconfig add Pool 11 size 100
```

Beispiel 28–8 Löschen des SPI

Im folgenden Beispiel wird gezeigt, wie Sie den SPI-Sicherheitsparameter `SPI 257` löschen

```
# mipagentconfig delete SPI 257
```

▼ So zeigen Sie die aktuellen Parameterwerte in der Konfigurationsdatei an

Geben Sie den Befehl `mipagentconfig get` ein, um die aktuellen Einstellungen anzuzeigen, die den Parameterzielen zugeordnet sind.

1 Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser auf dem System an, auf dem Sie Mobile IP aktivieren möchten.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Geben Sie für jeden Parameter, dessen Einstellungen angezeigt werden sollen, den folgenden Befehl ein:

```
# mipagentconfig get [<parameter> | <label>]
```

Wenn Sie beispielsweise die Advertisement-Einstellungen für das Gerät `hme0` anzeigen möchten, geben Sie den folgenden Befehl ein:

```
# mipagentconfig get adv hme0
```

Als Ergebnis könnte die folgende Ausgabe angezeigt werden:

```
[Advertisements hme0]
   HomeAgent = yes
   ForeignAgent = yes
```

Beispiel 28–9 Verwenden des Befehls `mipagentconfig get` zum Anzeigen von Parameterwerten

Im folgenden Beispiel ist das Ergebnis für den Befehl `mipagentconfig get` mit bestimmten Parameterzielen aufgeführt.

```
# mipagentconfig get MaxClockSkew
      [GlobalSecurityParameters]
         MaxClockSkew=300

# mipagentconfig get HA-FAauth
      [GlobalSecurityParameters]
         HA-FAauth=no

# mipagentconfig get MN-FAauth
      [GlobalSecurityParameters]
         MN-FAauth=no

# mipagentconfig get Challenge
      [GlobalSecurityParameters]
         Challenge=no

# mipagentconfig get Pool 10
      [Pool 10]
         BaseAddress=192.168.1.1
         Size=100

# mipagentconfig get SPI 257
      [SPI 257]
         Key=11111111111111111111111111111111
         ReplayMethod=none
```

```
# mipagentconfig get SPI 258
      [SPI 258]
         Key=15111111111111111111111111111111
         ReplayMethod=none

# mipagentconfig get addr 10.1.1.1
      [Address 10.1.1.1]
         SPI=258
         Type=agent

# mipagentconfig get addr 192.168.1.200
      [Address 192.168.1.200]
         SPI=257
         Type=node
```

Anzeigen des Mobility-Agent-Status

Geben Sie den Befehl `mipagentstat` ein, um die Besucherliste eines Foreign-Agent und die Bindungstabelle eines Home-Agent anzuzeigen. „Status des Mobile IP Mobility-Agent“ auf Seite 774 enthält eine konzeptuelle Beschreibung der Verwendung des Befehls `mipagentstat`. Lesen Sie auch die Manpage `mipagentstat`(1M).

▼ So zeigen Sie den Mobility-Agent-Status an

1 Melden Sie sich als Superuser oder mit einer entsprechenden Rolle beim System an, auf dem Sie Mobile IP aktivieren möchten.

Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2 Zeigen Sie den Mobility-Agent-Status an.

`# mipagentstat` *options*

`-f` Zeigt die Liste der aktiven mobilen Knoten in der Besucherliste des Foreign-Agent an.

`-h` Zeigte die Liste der aktiven mobilen Knoten in der Bindungstabelle des Home-Agent an.

`-p` Zeigt die Liste der Sicherheitszuordnungen mit den Mobility-Agent-Peers des Agenten an.

Beispiel 28–10 Anzeigen des Mobility-Agent-Status

Im folgenden Beispiel wird gezeigt, wie Sie die Besucherliste aller mobilen Knoten aufführen, die bei einem Foreign-Agent registriert sind.

```
# mipagentstat -f
```

Als Ergebnis wird eine Ausgabe ähnlich der Folgenden angezeigt:

```
Mobile Node     Home Agent     Time (s)     Time (s)  Flags
                               Granted      Remaining
--------------- -------------- ------------ --------- -----
foobar.xyz.com  ha1.xyz.com    600          125       .....T.
10.1.5.23       10.1.5.1       1000         10        .....T.
```

Als Ergebnis wird eine Ausgabe ähnlich der Folgenden angezeigt:

```
Foreign                  ..... Security Association(s).....
Agent                    Requests Replies  FTunnel  RTunnel
----------------------   -------- -------- -------- --------
forn-agent.eng.sun.com   AH       AH       ESP      ESP
```

Im folgenden Beispiel wird gezeigt, wie die Sicherheitszuordnungen eines Home-Agent aufgeführt werden.

```
# mipagentstat -fp
```

Als Ergebnis wird eine Ausgabe ähnlich der Folgenden angezeigt:

```
Home                     ..... Security Association(s) .....
Agent                    Requests Replies  FTunnel  RTunnel
----------------------   -------- -------- -------- --------
home-agent.eng.sun.com   AH       AH       ESP      ESP
ha1.xyz.com              AH,ESP   AH       AH,ESP   AH,ESP
```

Anzeigen der Mobility-Routen auf einem Foreign-Agent

Geben Sie den Befehl `netstat` ein, um zusätzliche Informationen über quellenspezifische Routen anzuzeigen, die von Vorwärts- und Rücktunneln erstellt werden. Weitere Informationen zu diesem Befehl finden Sie in der Manpage `netstat`(1M).

▼ So zeigen Sie die Mobility-Routen auf einem Foreign-Agent an

1. **Melden Sie sich als Superuser oder mit einer entsprechenden Rolle beim System an, auf dem Sie Mobile IP aktivieren möchten.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

2 Zeigen Sie die Mobility-Routen an.

```
# netstat -rn
```

Beispiel 28–11 Anzeigen der Mobility-Routen auf einem Foreign-Agent

Im folgenden Beispiel werden die Routen für einen Foreign-Agent angezeigt, der einen Rücktunnel verwendet.

```
Routing Table:   IPv4 Source-Specific
Destination      In If     Source      Gateway Flags  Use  Out If
-------------  ------- ------------ --------- -----  ---- -------
10.6.32.11     ip.tun1      --      10.6.32.97  UH      0 hme1
    --         hme1    10.6.32.11       --      U       0 ip.tun1
```

Die erste Zeile gibt an, dass die IP-Zieladresse `10.6.32.11` und die Eingangsschnittstelle `ip.tun1` die Schnittstelle `hme1` zum Weiterleiten der Pakete auswählen. Die nächste Zeile gibt an, dass alle Pakete von der Schnittstelle `hme1` und der Quelladresse `10.6.32.11` an `ip.tun1` weitergeleitet werden müssen.

◆ ◆ ◆ KAPITEL 29

Mobile IP-Dateien und Befehle (Referenz)

In diesem Kapitel werden die Komponenten beschrieben, die mit der Solaris-Implementierung von Mobile IP bereitgestellt werden. Um Mobile IP zu verwenden, müssen Sie zunächst die Mobile IP-Konfigurationsdatei konfigurieren. Dazu verwenden Sie die in diesem Kapitel beschriebenen Parameter und Befehle.

Dieses Kapitel enthält die folgenden Informationen:

- „Overview of the Solaris Mobile IP Implementation“ auf Seite 759
- „Mobile IP-Konfigurationsdatei“ auf Seite 760
- „Konfiguration des Mobility IP-Agent“ auf Seite 773
- „Status des Mobile IP Mobility-Agent“ auf Seite 774
- „Informationen zum Mobile IP-Status“ auf Seite 775
- „`netstat`-Erweiterungen für Mobile IP“ auf Seite 775
- „`snoop`-Erweiterungen für Mobile IP“ auf Seite 776

Hinweis – Die Mobile IP-Funktion ist in Solaris 10-Aktualisierungen nach Solaris 10 8/07 nicht mehr vorhanden.

Overview of the Solaris Mobile IP Implementation

Die Mobility-Agent-Software bietet Leistungsmerkmale des Home-Agent und des Foreign-Agent. Die Solaris Mobile IP-Software bietet keinen mobilen Clientknoten. Es wird nur der Agent-Leistungsumfang bereitgestellt. Jedes Netzwerk mit Mobility-Unterstützung muss über mindestens einen statischen (nicht-mobilen) Host verfügen, der diese Software ausführt.

In der Solaris-Umsetzung von Mobile IP werden die folgenden RFC-Funktionen unterstützt:

- RFC 1918, „Address Allocation for Private Internets“ (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`)
- RFC 2002, „IP Mobility Support“ (nur Agent) (`http://www.ietf.org/rfc/rfc2002.txt?number=2002`)

- RFC 2003, „IP Encapsulation Within IP" (http://www.ietf.org/rfc/rfc2003.txt?number=2003)
- RFC 2794, „Mobile IP Network Access Identifier Extension for IPv4" (http://www.ietf.org/rfc/rfc2794.txt?number=2794)
- RFC 3012, „Mobile IPv4 Challenge/Response Extensions" (http://www.ietf.org/rfc/rfc3012.txt?number=3012)
- RFC 3024, „Reverse Tunneling for Mobile IP" (http://www.ietf.org/rfc/rfc3024.txt?number=3024)

Das allgemeine Mobile IP-Protokoll (RFC 2002) befasst sich nicht mit dem Problem der skalierbaren Schlüsselverteilung und behandelt die Schlüsselverteilung als ein orthogonales Problem. Die Solaris Mobile IP-Software verwendet nur manuell konfigurierte Schlüssel, die in einer Konfigurationsdatei angegeben sind.

Die folgenden RFC-Funktionen werden in der Solaris-Umsetzung von Mobile IP nicht unterstützt:

- RFC 1701, „General Routing Encapsulation" (http://www.ietf.org/rfc/rfc1701.txt?number-1701)
- RFC 2004, „Minimal Encapsulation Within IP" (http://www.ietf.org/rfc/rfc2004.txt?number=2004)

Die folgenden Funktionen werden in der Solaris-Umsetzung von Mobile IP nicht unterstützt:

- Das Weiterleiten von Multicast-Verkehr oder Broadcast-Verkehr vom Home-Agent zum Foreign-Agent eines mobilen Knotens, der ein Foreign-Netzwerk besucht
- Das Routing von Broadcast- und Multicast-Datagrammen über einen Rücktunnel
- Private Care-Of-Adressen oder private Home-Agent-Adressen

Weitere Informationen finden Sie in der Manpage mipagent(1M).

Mobile IP-Konfigurationsdatei

Beim Booten liest der Befehl `mipagent` Konfigurationsinformationen aus der Konfigurationsdatei `/etc/inet/mipagent.conf` ein. Mobile IP verwendet die Konfigurationsdatei `/etc/inet/mipagent.conf` zum Initialisieren des Mobile IP-Mobility-Agent. Wenn der Mobility-Agent konfiguriert ist und eingesetzt wird, sendet er in regelmäßigen Abständen Router Advertisement-Nachrichten und antwortet auf Solicitation-Nachrichten zur Router-Erkennung sowie auf Mobile IP-Registrierungsnachrichten.

Eine Beschreibung der Dateiattribute finden Sie in der Manpage mipagent.conf(4) Eine Beschreibung der Nutzung dieser Datei finden Sie in der Manpage mipagent(1M).

Format der Konfigurationsdatei

Die Mobile IP-Konfigurationsdatei besteht aus mehreren Abschnitten. Jeder Abschnitt hat einen einmaligen Namen und ist in eckige Klammern eingeschlossen. Jeder Abschnitt enthält mindestens ein Label. Sie können den Label mithilfe der folgenden Syntax Werte zuweisen:

```
[Section_name]
     Label-name = value-assigned
```

„Abschnitte und Label in der Konfigurationsdatei“ auf Seite 764 enthält eine Beschreibung der Abschnittsnamen, Label und möglichen Werte.

Beispiele für die Konfigurationsdatei

Die standardmäßige Solaris-Installation enthält die folgenden Beispiel-Konfigurationsdateien in dem Verzeichnis `/etc/inet`:

- `mipagent.conf-sample` – Diese Datei enthält eine Beispielkonfiguration für einen Mobile IP-Agent, der den Leistungsumfang von Foreign-Agent und Home-Agent bereitstellt.
- `mipagent.conf.fa-sample` – Dieser Datei enthält eine Beispielkonfiguration für einen Mobile IP-Agent, der nur den Leistungsumfang eines Foreign-Agent bereitstellt.
- `mipagent.conf.ha-sample` – Dieser Datei enthält eine Beispielkonfiguration für einen Mobile IP-Agent, der nur den Leistungsumfang eines Home-Agent bereitstellt.

Diese Beispiel-Konfigurationsdateien enthalten die Adressen und Sicherheitseinstellungen eines mobilen Knotens. Bevor Sie Mobile IP implementieren können, müssen Sie eine Konfigurationsdatei mit der Bezeichnung `mipagent.conf` erstellen und in dem Verzeichnis `/etc/inet` speichern. Diese Datei enthält die Konfigurationseinstellungen, die Ihre Anforderungen an eine Mobile IP-Umsetzung erfüllen. Sie können auch eine der Beispiel-Konfigurationsdateien wählen und die Adress- und Sicherheitsangaben durch Ihre Angaben ersetzen und die Datei dann nach `/etc/inet/mipagent.conf` kopieren.

Weitere Informationen finden Sie unter „So erstellen Sie eine Mobile IP-Konfigurationsdatei“ auf Seite 745.

`mipagent.conf-sample`-Datei

Das folgende Listing zeigt die Abschnitte, Label und Werte in der Datei `mipagent.conf-sample`. „Abschnitte und Label in der Konfigurationsdatei“ auf Seite 764 enthält eine Beschreibung der Syntax, Abschnitte, Label und Werte.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
```

```
   HomeAgent = yes
   ForeignAgent = yes
   PrefixFlags = yes
   AdvertiseOnBcast = yes
   RegLifetime = 200
   AdvLifetime = 200
   AdvFrequency = 5
   ReverseTunnel = no
   ReverseTunnelRequired = no

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[Pool 1]
   BaseAddress = 10.68.30.7
   Size = 4

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address mobilenode@sun.com]
   Type = node
   SPI = 257
   Pool = 1

[Address Node-Default]
   Type = node
   SPI = 258
   Pool = 1

[Address 10.68.30.36]
   Type = agent
   SPI = 257
```

`mipagent.conf.fa-sample`-Datei

Das folgende Listing zeigt die Abschnitte, Label und Werte in der Datei `mipagent.conf.fa-sample`. „Abschnitte und Label in der Konfigurationsdatei“ auf Seite 764 enthält eine Beschreibung der Syntax, Abschnitte, Label und Werte.

Die Datei `mipagent.conf.fa-sample` ist eine Konfigurationsdatei, die nur den Leistungsumfang eines Foreign-Agent bereitstellt. Diese Beispieldatei enthält keinen `Pool`-Abschnitt, da Pools nur von einem Home-Agent verwendet werden. Ansonsten entspricht diese Dateien der Datei `mipagent.conf-sample`.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
   HomeAgent = no
   ForeignAgent = yes
   PrefixFlags = yes
   AdvertiseOnBcast = yes
   RegLifetime = 200
   AdvLifetime = 200
   AdvFrequency = 5
   ReverseTunnel = yes
   ReverseTunnelRequired = no

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address 10.68.30.36]
   Type = agent
   SPI = 257
```

mipagent.conf.ha-sample-Datei

Das folgende Listing zeigt die Abschnitte, Label und Werte in der Datei mipagent.conf.ha-sample. „Abschnitte und Label in der Konfigurationsdatei" auf Seite 764 enthält eine Beschreibung der Syntax, Abschnitte, Label und Werte.

Die Datei mipagent.conf.ha-sample ist eine Konfigurationsdatei, die nur den Leistungsumfang eines Home-Agent bereitstellt. Ansonsten entspricht diese Dateien der Datei mipagent.conf-sample.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
   HomeAgent = yes
   ForeignAgent = no
   PrefixFlags = yes
   AdvertiseOnBcast = yes
   RegLifetime = 200
```

```
   AdvLifetime = 200
   AdvFrequency = 5
   ReverseTunnel = yes
   ReverseTunnelRequired = no

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[Pool 1]
   BaseAddress = 10.68.30.7
   Size = 4

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address mobilenode@sun.com]
   Type = node
   SPI = 257
   Pool = 1

[Address Node-Default]
   Type = node
   SPI = 258
   Pool = 1
```

Abschnitte und Label in der Konfigurationsdatei

Die Mobile IP-Konfigurationsdatei enthält die folgenden Abschnitte:

- `General` (Erforderlich)
- `Advertisements` (Erforderlich)
- `GlobalSecurityParameters` (Optional)
- `Pool` (Optional)
- `SPI` (Optional)
- `Address` (Optional)

Die Abschnitte `General` und `GlobalSecurityParameters` enthalten Informationen für den Betrieb des Mobile IP-Agent. Diese Abschnitte können nur einmal in einer Konfigurationsdatei erscheinen.

General

Der Abschnitt General enthält nur ein Label: die Versionsnummer der Konfigurationsdateien. Der Abschnitt General weist die folgende Syntax auf:

```
[General]
     Version = 1.0
```

Advertisements

Der Abschnitt Advertisements enthält die Label HomeAgent und ForeignAgent sowie weitere Label. Sie müssen für jede Schnittstelle auf dem lokalen Host, der Mobile IP-Services bereitstellt, einen eigenen Advertisements-Abschnitt einfügen. Der Abschnitt Advertisements weist die folgende Syntax auf:

```
[Advertisements interface]
     HomeAgent = <yes/no>
     ForeignAgent = <yes/no>
     .
     .
```

In der Regel verfügt Ihr System über eine Schnittstelle, z. B. eri0 oder hme0, und unterstützt sowohl Home-Agent- als auch Foreign-Agent-Vorgänge. Diese Situation für das Beispiel hme0 vorausgesetzt, wird den beiden Label HomeAgent und ForeignAgent der Wert yes zugeordnet:

```
[Advertisements hme0]
     HomeAgent = yes
     ForeignAgent = yes
     .
     .
```

Bei Advertisement-Nachrichten über dynamische Schnittstellen verwenden Sie '*' als Geräte-ID-Komponente. Beispielsweise weist *Schnittstellenname* ppp* darauf hin, dass alle PPP-Schnittstellen erst nach dem Start des mipagent-Daemon konfiguriert wurden. Alle Attribute im Advertisement-Abschnitt bleiben bei einer dynamischen Schnittstelle gleich.

In der folgenden Tabelle sind die Label und Werte aufgeführt, die Sie im Abschnitt Advertisements verwenden können.

TABELLE 29–1 Advertisements-Abschnitt, Label und Werte

Bezeichnung	Wert	Beschreibung
HomeAgent	yes oder no	Legt fest, ob der mipagent-Daemon die Funktionen eines Home-Agent bereitstellt.
ForeignAgent	yes oder no	Legt fest, ob der mipagent-Daemon die Funktionen eines Foreign-Agent bereitstellt.
PrefixFlags	yes oder no	Gibt an, ob Advertisements die optionale Erweiterung für die Präfixlänge enthalten.

TABELLE 29–1 Advertisements-Abschnitt, Label und Werte *(Fortsetzung)*

Bezeichnung	Wert	Beschreibung
AdvertiseOnBcast	yes oder no	Bei yes können Advertisements über 255.255.255.255 anstelle von 224.0.0.1 gesendet werden.
RegLifetime	n	Die maximale Lebensdauer in Sekunden, die in Registrierungsanforderungen akzeptiert wird.
AdvLifetime	n	Die maximale Zeit in Sekunden, die eine Advertisement-Nachricht bei Nichtvorhandensein weiterer Advertisement-Nachrichten als gültig angesehen wird.
AdvFrequency	n	Die Zeit in Sekunden zwischen zwei aufeinander folgenden Advertisement-Nachrichten.
ReverseTunnel	yes oder noFA oder HA oder both	Legt fest, ob mipagent die Funktionen eines Rücktunnels bereitstellt. Der Wert yes bedeutet, dass sowohl Foreign-Agent als auch Home-Agent einen Rücktunnel unterstützen. Der Wert no bedeutet, dass die Schnittstelle keinen Rücktunnel unterstützt. Der Wert FA bedeutet, dass der Foreign-Agent einen Rücktunnel unterstützt. Der Wert HA bedeutet, dass der Home-Agent einen Rücktunnel unterstützt. Der Wert both bedeutet, dass sowohl Foreign-Agent als auch Home-Agent einen Rücktunnel unterstützen.
ReverseTunnelRequired	yes oder no	Legt fest, ob mipagent die Funktionen eines Rücktunnels erfordert. Legt entsprechend fest, ob ein mobiler Knoten während der Registrierung einen Rücktunnel benötigt. Der Wert yes bedeutet, dass sowohl Foreign-Agent als auch Home-Agent einen Rücktunnel benötigen. Der Wert no bedeutet, dass die Schnittstelle keinen Rücktunnel benötigt. Der Wert FA bedeutet, dass der Foreign-Agent einen Rücktunnel benötigt. Der Wert HA bedeutet, dass der Home-Agent einen Rücktunnel benötigt.
AdvInitCount	n	Legt den Anfangswert von unaufgeforderten Advertisement-Nachrichten fest. Der Standardwert ist 1. Der Wert wird nur berücksichtigt, wenn AdvLimitUnsolicited auf yes gesetzt ist.

TABELLE 29–1 `Advertisements`-Abschnitt, Label und Werte *(Fortsetzung)*

Bezeichnung	Wert	Beschreibung
`AdvLimitUnsolicited`	yes oder no	Aktiviert oder deaktiviert eine eingeschränkte Anzahl an unaufgeforderten Advertisement-Nachrichten über die Mobility-Schnittstelle.

`GlobalSecurityParameters`

Der Abschnitt `GlobalSecurityParameters` enthält die Label `maxClockSkew`, `HA-FAauth`, `MN-FAauth`, `Challenge` und `KeyDistribution`. Dieser Abschnitt weist die folgende Syntax auf:

```
[GlobalSecurityParameters]
     MaxClockSkew = n
     HA-FAauth = <yes/no>
     MN-FAauth = <yes/no>
     Challenge = <yes/no>
     KeyDistribution = files
```

Das Mobile IP-Protokoll bietet einen Replay-Schutz, indem es Zeitmarken in die Nachrichten aufnimmt. Wenn die Zeiten abweichen, sendet der Home-Agent eine Fehlermeldung mit der aktuellen Zeit an den mobilen Knoten zurück, und der mobile Knoten kann unter Verwendung der aktuellen Zeit eine erneute Registrierung versuchen. Mit dem Label `MaxClockSkew` konfigurieren Sie die maximale Anzahl an Sekunden, um die die Uhren des Home-Agent und des mobilen Knoten abweichen dürfen. Der Standardwert beträgt 300 Sekunden.

Mit den Label `HA-FAauth` und `MN-FAauth` aktivieren oder deaktivieren Sie eine Anforderung nach einer Home-Foreign- und einer Mobile-Foreign-Authentifizierung. Der Standardwert ist deaktiviert. Mit dem Label `challenge` können Sie konfigurieren, dass bei Problemen am Foreign-Agent der mobile Knoten in seinen Advertisement-Nachrichten gefordert wird. Dieses Label dient als Replay-Schutz. Auch hier lautet der Standardwert deaktiviert.

In der folgenden Tabelle sind die Label und Werte aufgeführt, die Sie im Abschnitt `GlobalSecurityParameters` verwenden können.

TABELLE 29–2 `GlobalSecurityParameters` -Abschnitt, Label und Werte

Bezeichnung	Wert	Beschreibung
`MaxClockSkew`	`n`	Die Anzahl an Sekunden, die `mipagent` als Abweichung zwischen der eigenen lokalen Zeit und der Zeit in den Registrierungsanforderungen akzeptiert.
`HA-FAauth`	yes oder no	Gibt an, ob HA-FA-Authentifizierungserweiterungen in den Registrierungsanforderungen und -antworten enthalten sein müssen.
`MN-FAauth`	yes oder no	Gibt an, ob MN-FA-Authentifizierungserweiterungen in den Registrierungsanforderungen und -antworten enthalten sein müssen.

TABELLE 29–2 `GlobalSecurityParameters` -Abschnitt, Label und Werte *(Fortsetzung)*

Bezeichnung	Wert	Beschreibung
`Challenge`	`yes` oder `no`	Gibt an, ob der Foreign-Agent Herausforderungen in seine Mobility Advertisement-Nachrichten aufnimmt.
`KeyDistribution`	`files`	Muss auf „files“ gesetzt sein.

Pool

Mobilen Knoten können vom Home-Agent dynamische Adressen zugewiesen werden. Die dynamische Adresszuweisung erfolgt unabhängig von DHCP innerhalb des `mipagent`-Daemon. Sie können einen Adresspool erstellen, der von mobilen Knoten verwendet wird, die eine Home-Adresse anfordern. Adresspools werden im `Pool`-Abschnitt der Konfigurationsdatei konfiguriert.

Der Abschnitt `Pool` enthält die Label `BaseAddress` und `Size.` Der Abschnitt `Pool` weist die folgende Syntax auf:

```
[Pool pool-identifier]
     BaseAddress = IP-address
     Size = size
```

Hinweis – Wenn Sie einen `Pool`-Bezeichner verwenden, muss dieser auch im Abschnitt `Address` des mobilen Knotens vorhanden sein.

In dem Abschnitt `Pool` definieren Sie Adresspools, die den mobilen Knoten zugewiesen werden können. Mit dem Label `BaseAddress` richten Sie die erste IP-Adresse im Pool ein. Mit dem Label `Size` geben Sie die Anzahl an Adressen an, die im Pool verfügbar sind.

Wenn beispielsweise die IP-Adressen `192.168.1.1` bis `192.168.1.100` im Pool 10 reserviert sind, enthält der Abschnitt `Pool` den folgenden Eintrag:

```
[Pool 10]
     BaseAddress = 192.168.1.1
     Size = 100
```

Hinweis – Die Adressbereiche sollten die Broadcast-Adresse nicht einbeziehen. Beispielsweise sollten Sie nicht `BaseAddress = 192.168.1.200` und `Size = 60` zuweisen, da dieser Bereich die Broadcast-Adresse `192.168.1.255` enthält.

In der folgenden Tabelle sind die Label und Werte aufgeführt, die im Abschnitt `Pool` verwenden werden können.

TABELLE 29–3 `Pool`-Abschnitt, Label und Werte

Bezeichnung	Wert	Beschreibung
`BaseAddress`	`n.n.n.n`	Die erste Adresse im Adresspool.
`Size`	`n`	Anzahl der Adressen im Pool.

SPI

Da das Mobile IP-Protokoll eine Nachrichtenauthentifizierung erfordert, müssen Sie den Sicherheitskontext mithilfe eines Security Parameter Index (SPI) identifizieren. Sie definieren den Sicherheitskontext im Abschnitt `SPI.` Sie müssen für jeden definierten Sicherheitskontext einen eigenen `SPI`-Abschnitt einfügen. Der Sicherheitskontext wird durch eine nummerische ID gekennzeichnet. Das Mobile IP-Protokoll reserviert die ersten 256 SPIs. Aus diesem Grunde sollten Sie nur SPI-Werte über 256 verwenden. Der Abschnitt `SPI` enthält sicherheitsbezogene Informationen wie Shared Secrets und Replay-Schutz.

Der Abschnitt `SPI` enthält darüber hinaus die Label `ReplayMethod` und `Key.` Der Abschnitt `SPI` weist die folgende Syntax auf:

```
[SPI SPI-identifier]
     ReplayMethod = <none/timestamps>
     Key = key
```

Zwei kommunizierende Peers müssen den gleichen SPI-Bezeichner verwenden. Sie müssen die Peers mit dem gleichen Schlüssel und der gleichen Wiedergabemethode konfigurieren. Den Schlüssel geben Sie als einen String mit hexadezimalen Zeichen ein. Die maximale Länge beträgt 16 Byte. Wenn der Schlüssel 16 Byte lang ist und die hexadezimalen Werte von `0` bis `f` enthält, könnte der Schlüssel-String wie folgt aussehen:

```
Key = 0102030405060708090a0b0c0d0e0f10
```

Der Schlüssel muss eine gerade Anzahl an Zeichen aufweisen, entsprechend den zwei Ziffern pro Byte-Darstellung.

In der folgenden Tabelle sind die Label und Werte aufgeführt, die Sie im Abschnitt `SPI` verwenden können.

TABELLE 29–4 `SPI`-Abschnitt, Label und Werte

Bezeichnung	Wert	Beschreibung
`ReplayMethod`	`none` oder `timestamps`	Gibt die Art der für die SPI verwendeten Authentifizierung für ein Replay an.
`Key`	`x`	Authentifizierungsschlüssel in hexadezimaler Form.

Address

In der Solaris-Implementierung von Mobile IP können Sie drei verschiedene Methoden zur Konfiguration von mobilen Knoten wählen. Jede Methode wird im Abschnitt `Address` konfiguriert. Die erste Methode folgt dem traditionellen Mobile IP-Protokoll und erfordert, dass jeder mobile Knoten über eine Home-Adresse verfügt. Bei der zweiten Methode wird ein mobiler Knoten über dessen Network Access Identifier (NAI) identifiziert. Beim letzten Verfahren konfigurieren Sie einen *standardmäßigen* mobilen Knoten, der von jedem mobilen Knoten verwendet werden kann, der über einen korrekten SPI-Wert und entsprechendes Schlüsselmaterial verfügt.

Mobiler Knoten

Der Abschnitt `Address` eines mobilen Knotens enthält die Label `Type` und `SPI`, mit denen der Adresstyp und der SPI-Bezeichner definiert werden. Der Abschnitt `Address` weist die folgende Syntax auf:

```
[Address address]
     Type = node
     SPI = SPI-identifier
```

Für jeden unterstützten mobilen Knoten müssen Sie einen `Address`-Abschnitt in die Konfigurationsdatei eines Home-Agent einfügen.

Wenn eine Mobile IP-Nachrichtenauthentifizierung zwischen Foreign-Agent und Home-Agent erforderlich ist, müssen Sie einen `Address`-Abschnitt für jeden Peer aufnehmen, mit dem ein Agent kommunizieren muss.

Der von Ihnen konfigurierte SPI-Wert muss einen in der Konfigurationsdatei vorhandenen `SPI`-Abschnitt darstellen.

Sie können auch private Adressen für einen mobilen Knoten konfigurieren.

In der folgenden Tabelle sind die Label und Werte aufgeführt, die Sie im Abschnitt `Address` für einen mobilen Knoten verwenden können.

TABELLE 29–5 `Address`-Abschnitt, Label und Werte (mobiler Knoten)

Bezeichnung	Wert	Beschreibung
`Type`	`Knoten`	Gibt an, dass der Eintrag für einen mobilen Knoten gilt.
`SPI`	`n`	Gibt den SPI-Wert für den zugehörigen Eintrag an.

Mobility-Agent

Der Abschnitt `Address` eines Mobility-Agent enthält die Label `Type` und `SPI`, mit denen der Adresstyp und der SPI-Bezeichner definiert werden. Der Abschnitt `Address` für einen Mobility-Agenten besitzt die folgende Syntax:

```
[Address address]
     Type = agent
     SPI = SPI-identifier
```

Für jeden unterstützten Mobilty-Agent müssen Sie einen `Address`-Abschnitt in die Konfigurationsdatei eines Home-Agent einfügen.

Wenn eine Mobile IP-Nachrichtenauthentifizierung zwischen Foreign-Agent und Home-Agent erforderlich ist, müssen Sie einen `Address`-Abschnitt für jeden Peer aufnehmen, mit dem ein Agent kommunizieren muss.

Der von Ihnen konfigurierte SPI-Wert muss einen in der Konfigurationsdatei vorhandenen `SPI`-Abschnitt darstellen.

In der folgenden Tabelle sind die Label und Werte aufgeführt, die Sie im Abschnitt `Address` für einen Mobility-Agent verwenden können.

TABELLE 29–6 `Address`-Abschnitt, Label und Werte (Mobility-Agent)

Bezeichnung	Wert	Beschreibung
`Type`	`agent`	Gibt an, dass der Eintrag für einen Mobility-Agent gilt.
`SPI`	`n`	Gibt den SPI-Wert für den zugehörigen Eintrag an.

Mobiler Knoten, der durch seinen NAI identifiziert wird

Der `Address`-Abschnitt eines mobilen Knotens, der durch seinen NAI identifiziert wird, enthält die Label `Type`, `SPI` und `Pool.` Mit dem NAI-Parameter können Sie mobile Knoten über deren NAI identifizieren. Der Abschnitt `Address` weist bei Verwendung des NAI-Parameters die folgende Syntax auf:

```
[Address NAI]
     Type = Node
     SPI = SPI-identifier
     Pool = pool-identifier
```

Zum Arbeiten mit Pools identifizieren Sie mobile Knoten über deren NAI. Mit dem Abschnitt `Address` können Sie einen NAI konfigurieren. Dies ist mit einer Home-Adresse nicht möglich. Ein NAI verwendet das Format `Benutzer@Domäne`. Mit dem Label `Pool` geben Sie den Adresspool an, der zum Zuweisen der Home-Adresse zum mobilen Knoten verwendet wird.

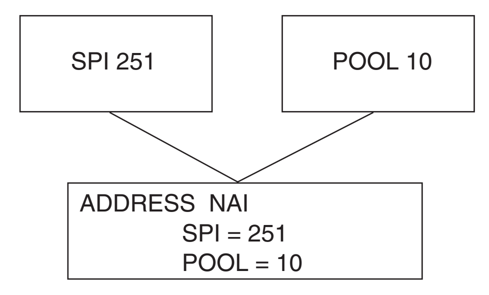
In der folgenden Tabelle sind die Label und Werte aufgeführt, die Sie im Abschnitt `Address` eines mobilen Knotens verwenden können, der durch seinen NAI identifiziert wird.

TABELLE 29–7 Address-Abschnitt, Label und Werte (mobiler Knoten, der durch seinen NAI identifiziert wird)

Bezeichnung	Wert	Beschreibung
Type	Knoten	Gibt an, dass der Eintrag für einen mobilen Knoten gilt.
SPI	n	Gibt den SPI-Wert für den zugehörigen Eintrag an.
Pool	n	Weist den Pool zu, aus dem einem mobilen Knoten eine Adresse zugewiesen wird.

Es müssen entsprechende SPI- und Pool-Abschnitte für die Label SPI und Pool vorhanden sein, die im durch den NAI identifizierten Address-Abschnitt eines mobilen Knotens definiert sind. Dies wird in der folgenden Abbildung verdeutlicht.

ABBILDUNG 29–1 Entsprechende SPI- und Pool-Abschnitte für den Address-Abschnitt bei einem mobilen Knoten, der durch seinen NAI identifiziert wird



Standardmäßiger mobiler Knoten

Der Address-Abschnitt eines standardmäßigen mobilen Knotens enthält die Label Type, SPI und Pool. Mit dem Parameter Node-Default können Sie allen mobilen Knoten gestatten, einen Service zu beziehen, sofern sie den richtigen SPI aufweisen (definiert in diesem Abschnitt). Der Abschnitt Address weist bei Verwendung des Node-Default-Parameters die folgende Syntax auf:

```
[Address Node-Default]
     Type = Node
     SPI = SPI-identifier
     Pool = pool-identifier
```

Mit dem Parameter Node-Default können Sie die Größe der Konfigurationsdatei verringern. Andernfalls muss für jeden mobilen Knoten ein eigener Abschnitt vorhanden sein. Der Node-Default-Parameter stellt jedoch ein Sicherheitsrisiko dar. Wenn einem mobilen Knoten aus beliebigen Gründen nicht mehr vertraut wird, müssen Sie die Sicherheitsinformationen auf allen vertrauenswürdigen mobilen Knoten aktualisieren. Diese Aufgabe kann sehr aufwändig

werden. Sie können den `Node-Default`-Parameter jedoch in Netzwerken verwenden, in denen Sicherheitsrisiken als vernachlässigbar angesehen werden.

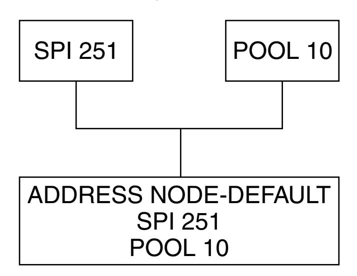
In der folgenden Tabelle sind die Label und Werte aufgeführt, die Sie im Abschnitt `Address` für einen standardmäßigen mobilen Knoten verwenden können.

TABELLE 29–8 `Address`-Abschnitt, Label und Werte (standardmäßiger mobiler Knoten)

Bezeichnung	Wert	Beschreibung
`Type`	`Knoten`	Gibt an, dass der Eintrag für einen mobilen Knoten gilt.
`SPI`	`n`	Gibt den SPI-Wert für den zugehörigen Eintrag an.
`Pool`	`n`	Weist den Pool zu, aus dem einem mobilen Knoten eine Adresse zugewiesen wird.

Es müssen entsprechende `SPI`- und `Pool`-Abschnitte für die Label `SPI` und `Pool` vorhanden sein, die im `Address`-Abschnitt eines standardmäßigen mobilen Knotens definiert sind. Dies wird in der folgenden Abbildung verdeutlicht.

ABBILDUNG 29–2 Entsprechende `SPI`- und `Pool`-Abschnitte für den Address-Abschnitt bei einem standardmäßigen mobilen Knoten



Konfiguration des Mobility IP-Agent

Mit dem Befehl `mipagentconfig` konfigurieren Sie den Mobility-Agent. Dabei können Sie jeden Parameter in der Konfigurationsdatei `/etc/inet/mipagent.conf` erstellen oder ändern. Außerdem können Sie jede Einstellung ändern, und Mobility-Clients, Pools und SPIs hinzufügen oder löschen. Der Befehl `mipagentconfig` weist die folgende Syntax auf:

```
# mipagentconfig <command> <parameter> <value>
```

In der folgenden Tabelle sind die Befehle aufgeführt, die Sie mit `mipagentconfig` zum Erstellen oder Ändern von Parametern in der Konfigurationsdatei `/etc/inet/mipagent.conf` verwenden können.

TABELLE 29–9 `mipagentconfig`-Unterbefehle

Befehl	Beschreibung
`add`	Dient zum Hinzufügen von Advertisement-Parametern, Sicherheitsparametern, SPIs und Adressen zur Konfigurationsdatei.
`change`	Dient zum Ändern von Advertisement-Parametern, Sicherheitsparametern, SPIs und Adressen in der Konfigurationsdatei.
`delete`	Dient zum Löschen von Advertisement-Parametern, Sicherheitsparametern, SPIs und Adressen aus der Konfigurationsdatei.
`get`	Dient zum Anzeigen der aktuellen Werte in der Konfigurationsdatei.

Eine Beschreibung der Befehlsparameter sowie der zulässigen Werte finden Sie in der Manpage `mipagentconfig(1M)` „Ändern einer Mobile IP-Konfigurationsdatei" auf Seite 749 beschreibt Verfahren, die Sie mit dem Befehl `mipagentconfig` verwenden können.

Status des Mobile IP Mobility-Agent

Geben Sie den Befehl `mipagentstat` ein, um die Besucherliste eines Foreign-Agent und die Bindungstabelle eines Home-Agent anzuzeigen. Sie können auch die Liste der Sicherheitszuordnungen mit den Mobility-Agent-Peers des Agenten anzeigen. Für die Besucherliste eines Foreign-Agent geben Sie den Befehl `mipagentstat` mit der Option `-f` ein. Um die Bindungstabelle eines Home-Agent anzuzeigen, geben Sie den Befehl `mipagentstat` mit der Option `-h` ein. Die folgenden Beispiele zeigen die typische Ausgabe, wenn der Befehl `mipagentstat` mit diesen Optionen verwendet wird.

BEISPIEL 29–1 Besucherliste eines Foreign-Agent

```
Mobile Node     Home Agent     Time (s)     Time (s)  Flags
                               Granted      Remaining
--------------- -------------- ------------ --------- -----
foobar.xyz.com  ha1.xyz.com    600          125       .....T.
10.1.5.23       10.1.5.1       1000         10        .....T.
```

BEISPIEL 29–2 Bindungstabelle eines Home-Agent

```
Mobile Node     Home Agent     Time (s)     Time (s)  Flags
                               Granted      Remaining
--------------- -------------- ------------ --------- -----
foobar.xyz.com  fa1.tuv.com    600          125       .....T.
10.1.5.23       123.2.5.12     1000         10        .....T.
```

Weitere Informationen zu den Befehlsoptionen finden Sie in der Manpage `mipagentstat(1M)` „Anzeigen des Mobility-Agent-Status" auf Seite 756 beschreibt Verfahren, die Sie mit dem Befehl `mipagentstat` verwenden können.

Informationen zum Mobile IP-Status

Beim Herunterfahren speichert der mipagent-Daemon interne Statusinformationen in der Datei /var/inet/mipagent_state. Dies findet jedoch nur dann statt, wenn der mipagent-Daemon Services als Home-Agent bereitstellt. Die Statusinformationen umfassen die Liste der mobilen Knoten, die als Home-Agent unterstützt werden, deren aktuelle Care-Of-Adressen sowie die verbleibenden Registrierungslebensdauern. Darüber hinaus umfassen sie die Konfiguration der Sicherheitszuordnungen mit den Mobility-Agent-Peers. Wenn der mipagent für Wartungszwecke beendet und neu gestartet wird, wird der interne Status des Mobility-Agents mit der Datei mipagent_state weitestgehend wiederhergestellt. Die Absicht ist, die Serviceunterbrechung für mobile Knoten, die anderen Netzwerke besuchen, zu minimieren. Wenn die Datei mipagent_state existiert, wird sie unmittelbar nach mipagent.conf eingelesen, wenn der mipagent-Daemon gestartet oder neugestartet wird.

netstat-Erweiterungen für Mobile IP

Dem Befehl netstat wurden Mobile IP-Erweiterungen hinzugefügt, um Mobile IP-Weiterleitungsrouten zu identifizieren. Insbesondere können Sie mit dem Befehl netstat eine neue Routing-Tabelle anzeichnen, die als „Source-Specific " (quellenspezifisch) bezeichnet wird. Weitere Informationen finden Sie in der Manpage netstat(1M).

Im folgenden Beispiel wird die Ausgabe des Befehls netstat bei Verwendung der Flags -nr gezeigt.

BEISPIEL 29–3 Mobile IP-Ausgabe des Befehls netstat

```
Routing Table:   IPv4 Source-Specific
Destination      In If     Source      Gateway Flags  Use  Out If
--------------  ------- ------------ --------- -----  ---- -------
10.6.32.11      ip.tun1      --      10.6.32.97  UH      0 hme1
    --          hme1    10.6.32.11       --      U       0 ip.tun1
```

Im Beispiel werden die Routen für einen Foreign-Agent angezeigt, der einen Rücktunnel verwendet. Die erste Zeile gibt an, dass die IP-Zieladresse 10.6.32.11 und die Eingangsschnittstelle ip.tun1 die Schnittstelle hme1 zum Weiterleiten der Pakete auswählen. Die nächste Zeile gibt an, dass alle Pakete von der Schnittstelle hme1 und der Quelladresse 10.6.32.11 an ip.tun1 weitergeleitet werden müssen.

snoop-Erweiterungen für Mobile IP

Dem Befehl snoop wurden Mobile IP-Erweiterungen hinzugefügt, um den Mobile IP-Verkehr auf dem Link zu identifizieren. Weitere Informationen finden Sie in der Manpage snoop(1M).

Im folgenden Beispiel wird die Ausgabe des Befehls snoop gezeigt, der auf dem mobilen Knoten mip-mn2 ausgeführt wird.

BEISPIEL 29–4 Mobile IP-Ausgabe des Befehls snoop

```
mip-mn2# snoop
Using device /dev/hme (promiscuous mode)
  mip-fa2 -> 224.0.0.1    ICMP Router advertisement (Lifetime 200s [1]:
{mip-fa2-80 2147483648}), (Mobility Agent Extension), (Prefix Lengths),
(Padding)
  mip-mn2 -> mip-fa2   Mobile IP reg rqst
  mip-fa2 -> mip-mn2   Mobile IP reg reply (OK code 0)
```

In diesem Beispiel wird gezeigt, dass der mobile Knoten eine der regelmäßig vom Foreign-Agent mip-fa2 gesendeten Mobility Agent Advertisement-Nachrichten empfangen hat. Dann sendet mip-mn2 eine Registrierungsanforderung an mip-fa2 und empfängt eine Registrierungsantwort als Antwort. Die Registrierungsantwort kennzeichnet, dass der mobile Knoten erfolgreich bei seinem Home-Agent registriert wurde.

TEIL VI

IPMP

Dieser Teil enthält eine Einführung in das IP Network Multipathing (IPMP) und beschreibt Aufgaben zur Verwaltung von IPMP. IPMP bietet eine Ausfallerkennung und Failover für Schnittstellen auf einem System, die an den gleichen Link angeschlossen sind.

KAPITEL 30

Einführung in IPMP (Übersicht)

IP-Netzwerk-Multipathing (IPMP) bietet eine Erkennung von Ausfällen physikalischer Schnittstellen und transparentes Failover des Netzwerkzugriffs bei einem System mit mehreren Schnittstellen in der gleichen IP-Verbindung. Darüber hinaus bietet IPMP Lastverteilung von Paketen für Systeme mit mehreren Schnittstellen.

Dieses Kapitel enthält die folgenden Informationen:

- „Gründe für IPMP" auf Seite 779
- „Allgemeine Anforderungen von IPMP" auf Seite 783
- „IPMP-Adressierung" auf Seite 784
- „Oracle Solaris IPMP-Komponenten" auf Seite 780
- „IPMP-Schnittstellenkonfigurationen" auf Seite 787
- „IPMP-Funktionen zur Ausfall- und Reparaturerkennung" auf Seite 789
- „IPMP und Dynamische Rekonfiguration" auf Seite 793

Aufgaben zur Konfiguration von IPMP finden Sie in Kapitel 31, „Verwaltung von IPMP (Aufgaben)".

Gründe für IPMP

IPMP bietet Systemen mit mehreren physikalischen Schnittstellen Verbesserungen bei Zuverlässigkeit, Verfügbarkeit und Netzwerkleistung. Gelegentlich könnte eine physikalische Schnittstelle oder die an diese Schnittstelle angeschlossene Netzwerkhardware ausfallen oder Wartung erfordern. Früher konnte das System in diesem Fall nicht mehr über eine der IP-Adressen erreicht werden, die der ausgefallenen Schnittstelle zugewiesen sind. Darüber hinaus wurden alle bestehenden Verbindungen zu dem System unterbrochen, das diese IP-Adressen verwendet.

Mit IPMP können Sie eine oder mehrere physikalische Schnittstellen als eine IP Multipathing-Gruppe (oder *IPMP-Gruppe*) konfigurieren. Nach der Konfiguration von IPMP überwacht das System die Schnittstellen in der IPMP-Gruppe automatisch auf Ausfälle. Sollte

eine Schnittstelle in der Gruppe ausfallen oder zu Wartungszwecken deaktiviert werden, migriert IPMP automatisch die IP-Adressen der ausgefallenen Schnittstelle oder es findet ein *Failover* statt. Der Empfänger dieser Adressen wird eine ordnungsgemäß arbeitende Schnittstelle in der IPMP-Gruppe der ausgefallenen Schnittstelle. Die Failover-Funktion von IPMP erhält die Netzfähigkeit und verhindert eine Unterbrechung existierender Verbindungen. Darüber hinaus verbessert IPMP die allgemeine Leistung von Netzverbindungen, in dem Netzverkehr automatisch über das Schnittstellenset in der IPMP-Gruppe verteilt wird. Dieser Vorgang heißt *Lastverteilung*.

Oracle Solaris IPMP-Komponenten

Oracle Solaris IPMP umfasst die folgende Software:

- Den Daemon `in.mpathd`. Eine vollständige Beschreibung dieses Daemon finden Sie in der Manpage `in.mpathd`(1M).
- Die Konfigurationsdatei `/etc/default/mpathd`, die ebenfalls in der Manpage `in.mpathd`(1M) beschrieben wird.
- `ifconfig`-Optionen für die IPMP-Konfiguration (siehe Manpage `ifconfig`(1M)).

Multipathing-Daemon, `in.mpathd`

Der `in.mpathd`-Daemon erkennt Schnittstellenausfälle und implementiert dann verschiedene Verfahren zum Failover und Failback. Nachdem `in.mpathd` einen Ausfall oder eine vollzogene Reparatur erkannt hat, sendet der Daemon ein `ioctl`, um entweder Failover oder Failback durchzuführen. Das `ip`-Kernelmodul, das `ioctl` implementiert, führt den Netzwerkzugriff-Failover transparent und automatisch durch.

Hinweis – Verwenden Sie kein Alternate Pathing, so lange Sie IPMP auf dem gleichen Satz Netzwerkschnittstellenkarten verwenden. Entsprechend sollten Sie kein IPMP verwenden, wenn Sie Alternate Pathing einsetzen. Sie können jedoch Alternate Pathing und IPMP gleichzeitig auf unterschiedlichen Schnittstellensätzen anwenden. Weitere Informationen zum Alternate Pathing finden Sie im*Sun Enterprise Server Alternate Pathing 2.3.1 User Guide*.

Der `in.mpathd` erkennt Ausfälle und Reparaturen, in dem er Stichproben an alle Schnittstellen sendet, die zu einer IPMP-Gruppe gehören. Darüber hinaus erkennt der `in.mpathd`-Daemon Ausfälle und Reparaturen durch Überwachen des Flags `RUNNING` jeder Schnittstelle in der Gruppe. Weitere Informationen finden Sie in der Manpage `in.mpathd`(1M).

Hinweis – DHCP unterstützt die Verwaltung von IPMP-Datenadressen nicht. Wenn Sie versuchen, DHCP für diese Adressen zu verwenden, wird DHCP diese Adressen nicht mehr steuern. Verwenden Sie DHCP nicht für Datenadressen.

IPMP-Terminologie und Konzepte

In diesem Abschnitt werden Begriffe und Konzepte vorgestellt, die in den weiteren Kapiteln zum IPMP in diesem Handbuch verwendet werden.

IP-Link

In der IPMP-Terminologie ist ein *IP-Link* eine Kommunikationseinrichtung bzw. ein -medium, über das Knoten auf der Übertragungsschicht der Internet-Protokollfamilie kommunizieren können. Zu den IP-Links gehören einfache Ethernets, Bridged-Ethernets, Hubs oder Asynchronous Transfer Mode (ATM)-Netzwerke. Ein IP-Link kann über eine oder mehrere IPv4-Teilnetznummern, und, sofern anwendbar, über einen oder mehrere IPv6-Teilnetzpräfixe verfügen. Eine Teilnetznummer oder ein Präfix kann nur einen IP-Link zugeordnet werden. In ATM LANE ist ein IP-Link ein einzelnes, emuliertes Local Area Network (LAN). Beim Address Resolution Protocol (ARP) umfasst der Bereich des ARP-Protokolls einen IP-Link.

Hinweis – Andere IP-bezogene Dokumente wie z. B. RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, verwenden den Begriff *Link* anstelle von *IP-Link*. In Teil VI wird der Begriff *IP-Link* verwendet, um Verwechslungen mit IEEE 802 zu vermeiden. In IEEE 802 bezeichnet der Begriff *Link* eine einpolige Verbindung von einer Ethernet-Netzwerkschnittstellenkarte (NIC) zu einem Ethernet-Switch.

Physikalische Schnittstelle

Eine *physikalische Schnittstelle* sorgt für den Anschluss des Systems an einen IP-Link. Dieser Anschluss wird häufig als ein Gerätetreiber und eine NIC umgesetzt. Wenn Ihr System über mehrere Schnittstellen verfügt, die an den gleichen Link angeschlossen sind, können Sie IPMP so konfigurieren, dass beim Ausfall einer der Schnittstellen ein Failover stattfindet. Weitere Informationen zu physikalischen Schnittstellen finden Sie unter „IPMP-Schnittstellenkonfigurationen“ auf Seite 787.

Netzwerkschnittstellenkarte

Eine *Netzwerkschnittstelle* ist ein Netzwerkadapter, der in ein System integriert werden kann. Alternativ kann die NIC als separate Karte verwendet werden, die als Schnittstelle eines Systems mit einem IP-Link dient. Einige NICs verfügen über mehrere physikalische Schnittstellen. Beispielsweise kann eine `qfe`-NIC über vier Schnittstellen, `qfe0` bis `qfe3` verfügen.

IPMP-Gruppe

Eine IP-Multipathing-Gruppe (oder *IPMP*-Gruppe) setzt sich aus einer oder mehreren physikalischen Schnittstellen im gleichen System zusammen, die unter dem gleichen IPMP-Gruppennamen konfiguriert sind. Alle Schnittstellen in der IPMP-Gruppe müssen an den gleichen IP-Link angeschlossen sein. Alle Schnittstellen in der Gruppe sind durch den gleichen Zeichenstring (nicht-Null) für einen IPMP-Gruppennamen gekennzeichnet. Sie können Schnittstellen von NICs mit unterschiedlichen Geschwindigkeiten in die gleiche IPMP-Gruppe aufnehmen, solange die NICs den gleichen Typ aufweisen. Beispielsweise können Sie die Schnittstellen von 100-Megabit Ethernet-NICs und die Schnittstellen von 1-Gigabit Ethernet-NICs in die gleiche Gruppe aufnehmen. Ein anderes Beispiel geht von zwei 100-Megabit Ethernet-NICs aus. Sie können eine der Schnittstellen als 10-Megabit-NIC konfigurieren und dennoch beide Schnittstellen in die gleiche IPMP-Gruppe aufnehmen.

Es ist jedoch nicht möglich, zwei Schnittstellen unterschiedlichen Medientyps in eine IPMP-Gruppe aufzunehmen. So können Sie eine ATM-Schnittstelle nicht in die gleiche Gruppe wie eine Ethernet-Schnittstelle aufnehmen.

Ausfallerkennung und Failover

Ausfallerkennung ist der Prozess, wenn erkannt wird, dass eine Schnittstelle oder ein Pfad von einer Schnittstelle zu einem Gerät auf der Internetschicht nicht mehr funktioniert. IPMP bietet Systemen die Möglichkeit, den Ausfall einer Schnittstelle zu erkennen. IPMP kann die folgenden Arten von Kommunikationsausfällen erkennen:

- Der Sende- oder Empfangspfad einer Schnittstelle ist ausgefallen.
- Der Anschluss einer Schnittstelle zum IP-Link ist ausgefallen.
- Der Port am Switch sendet oder empfängt keine Pakete mehr.
- Die physikalische Schnittstelle in einer IPMP-Gruppe ist beim Systemstart nicht vorhanden.

Nach einem erkannten Ausfall leitet IPMP einen Failover-Prozess ein. *Failover* ist der automatische Prozess, den Netzwerkzugriff von einer ausgefallenen Schnittstelle auf eine funktionierende physikalische Schnittstelle in der gleichen Gruppe umzuschalten. Netzwerkzugriff umfasst IPv4 Unicast-, Multicast- und Broadcast-Verkehr sowie IPv6 Unicast- und Multicast-Verkehr. Failover kann nur dann stattfinden, wenn mindestens zwei Schnittstellen in der IPMP-Gruppe konfiguriert sind. Ein Failover-Prozess stellt unterbrechungsfreien Zugriff auf das Netzwerk sicher.

Reparaturerkennung und Failback

Bei einer *Reparaturerkennung* wird erfasst, dass eine NIC oder der Pfad von einer NIC zu einem Gerät auf der Internetschicht nach einem Ausfall wieder ordnungsgemäß funktioniert. Nachdem die Reparatur einer NIC erkannt wurde, führt IPMP ein *Failback* durch – der Prozess, bei dem der Netzwerkzugriff auf die reparierte Schnittstelle zurückgeschaltet wird. Für eine

Reparaturerkennung wird vorausgesetzt, dass Failbacks aktiviert worden sind. Weitere Informationen finden Sie unter „Erkennen der Reparatur physikalischer Schnittstellen“ auf Seite 791.

Zielsysteme

Die Stichproben-basierte Ausfallerkennung verwendet *Zielsysteme*, um den Zustand einer Schnittstelle zu ermitteln. Jedes Zielsystem muss an den gleichen IP-Link wie die Mitglieder der IPMP-Gruppe angeschlossen sein. Der `in.mpathd`-Daemon im lokalen System sendet ICMP-Stichprobennachrichten an alle Zielsysteme. Die Stichprobennachrichten helfen dabei, den Zustand jeder Schnittstelle in der IPMP-Gruppe zu ermitteln.

Weitere Informationen zu Zielsystemen, die bei der Stichproben-basierten Ausfallerkennung verwendet werden, finden Sie unter „Stichproben-basierte Ausfallerkennung“ auf Seite 790.

Abgehende Lastverteilung

Bei konfiguriertem IPMP werden abgehende Netzwerkpakete ohne Auswirkungen auf die Reihenfolge der Pakete auf mehrere NICs verteilt. Dieser Prozess wird als *Lastverteilung* bezeichnet. Durch eine Lastverteilung wird ein höherer Durchsatz im Netzwerk erreicht. Eine Lastverteilung tritt nur ein, wenn der Netzwerkverkehr über mehrere Verbindungen an mehrere Ziele fließt.

Dynamische Rekonfiguration

Dynamische Rekonfiguration (DR) ist die Fähigkeit, ein System im laufenden Zustand ohne oder mit nur geringen Auswirkungen auf vorhandene Vorgänge neu zu konfigurieren. Nicht alle Sun-Plattformen unterstützen DR. Einige Sun-Plattformen unterstützen DR nur bei bestimmten Hardwaretypen. Auf Plattformen, die die DR von NICs unterstützen, kann IPMP für transparentes Failover des Netzwerkzugriffs verwendet werden und so unterbrechungsfreien Netzwerkzugriff für das System bereitstellen.

Weitere Informationen, wie IPMP die DR unterstützt, finden Sie unter „IPMP und Dynamische Rekonfiguration“ auf Seite 793.

Allgemeine Anforderungen von IPMP

IPMP ist in Oracle Solaris integriert und benötigt keine spezielle Hardware. Jede Schnittstelle, die von Oracle Solaris unterstützt wird, kann mit IPMP verwendet werden. IPMP stellt jedoch die folgenden Anforderungen an Netzwerkkonfiguration und -topologie:

- Alle Schnittstellen in einer IPMP-Gruppe müssen über einmalige MAC-Adressen verfügen.

  Standardmäßig verwenden alle Netzwerkschnittstellen eines SPARC-basierten Systems eine gemeinsame MAC-Adresse. Daher müssen Sie die Standardeinstellung ändern, um IPMP auf SPARC-basierten Systemen verwenden zu können. Weitere Informationen hierzu finden Sie unter „So planen Sie für eine IPMP-Gruppe“ auf Seite 799.

- Alle Schnittstellen in einer IPMP-Gruppe müssen den gleichen Medientyp aufweisen. Weitere Informationen hierzu finden Sie unter „IPMP-Gruppe“ auf Seite 782.
- Alle Schnittstellen in einer IPMP-Gruppe müssen sich auf dem gleichen IP-Link befinden. Weitere Informationen hierzu finden Sie unter „IPMP-Gruppe“ auf Seite 782.

Hinweis – Mehrere IPMP-Gruppen auf derselben Sicherungsschicht-Broadcast-Domäne (L2 bzw. Layer 2) werden nicht unterstützt. Eine L2-Broadcast-Domäne ist normalerweise einem bestimmten Teilnetz zugeordnet. Sie müssen deshalb nur eine IPMP-Gruppe pro Teilnetz konfigurieren.

- Abhängig von Ihren Anforderungen an die Ausfallerkennung müssen Sie entweder bestimmte Netzwerkschnittstellen verwenden oder zusätzliche IP-Adressen für jede Netzwerkschnittstelle konfigurieren. Näheres finden Sie unter „Stichproben-basierte Ausfallerkennung“ auf Seite 789 und „Stichproben-basierte Ausfallerkennung“ auf Seite 790.

IPMP-Adressierung

Sie können die IPMP-Ausfallerkennung sowohl unter IPv4-Netzwerken und Dual-Stack IPv4- und IPv6-Netzwerken konfigurieren. Für IPMP konfigurierte Schnittstellen unterstützen zwei Arten von Adressen: Datenadressen und Testadressen.

Datenadressen

Datenadressen sind konventionelle IPv4- und IPv6-Adressen, die der Schnittstelle einer NIC entweder beim Booten oder manuell über den Befehl `ifconfig` zugewiesen wurden. Der standardmäßige IPv4- und, sofern anwendbar, IPv6-Paketverkehr über eine Schnittstelle wird als *Datenverkehr* angesehen.

Testadressen

Testadressen sind IPMP-spezifische Adressen, die vom `in.mpathd`-Daemon verwendet werden. Damit eine Schnittstelle Stichproben-basierte Ausfall- und Reparaturerkennung unterstützt, muss mindestens eine Testadresse für sie konfiguriert worden sein.

Hinweis – Testadressen müssen nur dann konfiguriert werden, wenn eine Stichproben-basierte Ausfallerkennung verwendet werden soll.

Der `in.mpathd`-Daemon verwendet Testadressen, um ICMP-Stichproben (so genannter *Stichprobenverkehr*) mit anderen Zielen auf dem IP-Link auszutauschen. Über den

Stichprobenverkehr kann der Status einer Schnittstelle und der dazugehörigen NIC ermittelt werden; so auch, ob eine Schnittstelle ausgefallen ist. Anhand der Stichprobenwerte wird überprüft, ob Sende- und Empfangspfad zur Schnittstelle ordnungsgemäß funktionieren.

Jede Schnittstelle kann mit einer IP-Testadresse konfiguriert werden. Für eine Schnittstelle in einem Dual-Stack-Netzwerk können Sie eine IPv4-Testadresse, eine IPv6-Testadresse oder sowohl IPv4- als auch IPv6-Testadressen konfigurieren.

Nach dem Ausfall einer Schnittstelle verbleiben die Testadressen bei der ausgefallenen Schnittstelle, so dass `in.mpathd` weiterhin Stichproben senden kann, um auf den Abschluss einer Reparatur zu prüfen. Sie müssen Testadressen gesondert konfigurieren, so dass sie nicht versehentlich von Anwendungen verwendet werden. Weitere Informationen hierzu finden Sie unter „Verwenden der Testadressen durch Anwendungen verhindern" auf Seite 786.

Weitere Informationen zur Stichproben-basierten Ausfallerkennung finden Sie unter „Stichproben-basierte Ausfallerkennung" auf Seite 790.

IPv4-Testadressen

Im Allgemeinen können Sie jede IPv4-Adresse in Ihren Teilnetz als Testadresse verwenden. IPv4-Testadressen müssen nicht routefähig sein. Da IPv4-Adressen an vielen Standorten nur beschränkt verfügbar sind, sollten Sie eventuell nicht-routefähige RFC 1918-Privatadressen als Testadressen verwenden. Beachten Sie, dass der `in.mpathd`-Daemon ICMP-Stichproben nur mit anderen Hosts im Teilnetz der Testadresse austauscht. Wenn Sie Testadressen im RFC 1918-Stil verwenden, müssen Sie darauf achten, andere Systeme (vorzugsweise Router) auf dem IP-Link mit Adressen im entsprechenden RFC 1918-Teilnetz zu konfigurieren. Erst dann kann der `in.mpathd`-Daemon Stichproben erfolgreich mit Zielsystemen austauschen.

Die IPMP-Beispiele verwenden RFC 1918-Adressen aus dem Netzwerk `192.168.0/24` als IPv4-Testadressen. Weitere Informationen zu privaten RFC 1918-Adressen finden Sie unter RFC 1918, Address Allocation for Private Internets. (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`)

Informationen zur Konfiguration von IPv4-Testadressen finden Sie unter „So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen" auf Seite 801.

IPv6-Testadressen

Die einzige gültige IPv6-Testadresse ist die Link-lokale Adresse einer physikalischen Schnittstelle. Für eine IPMP-Testadresse ist keine separate IPv6-Adresse erforderlich. Die Link-lokale Adresse basiert auf der Media Access Control (MAC)-Adresse der Schnittstelle. Link-lokale Adressen werden automatisch konfiguriert, wenn die Schnittstelle beim Booten oder manuell mithilfe des Befehls `ifconfig` für IPv6 aktiviert wird.

Zum Ermitteln der Link-lokalen Adresse einer Schnittstelle führen Sie den Befehl `ifconfig` *Schnittstelle* auf einem IPv6-aktivierten Knoten aus. Achten Sie auf die Ausgabe für die Adresse,

die mit dem Präfix `fe80` (dem Link-lokalen Präfix) beginnt. Das Flag `NOFAILOVER` in der folgenden `ifconfig`-Ausgabe zeigt, dass die Link-lokale Adresse `fe80::a00:20ff:feb9:17fa/10` der Schnittstelle `hme0` als Testadresse verwendet wird.

```
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
            inet6 fe80::a00:20ff:feb9:17fa/10
```

Weitere Informationen zu Link-lokalen Adressen finden Sie unter Link-lokale Unicast-Adresse.

Wenn eine IPMP-Gruppe sowohl IPv4 als auch IPv6 für alle Schnittstellen der Gruppe geplumbt (aktiviert) hat, müssen keine separaten IPv4-Testadressen mehr konfiguriert werden. Der `in.mpathd`-Daemon kann die Link-lokalen IPv6-Adressen als Testadressen verwenden.

Informationen zum Erstellen einer IPv6-Testadresse finden Sie unter „So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen“ auf Seite 801.

Verwenden der Testadressen durch Anwendungen verhindern

Nachdem Sie eine Testadresse konfiguriert haben, müssen Sie sicherstellen, dass diese Adresse nicht von Anwendungen verwendet wird. Andernfalls ist die Anwendung bei einem Ausfall der Schnittstelle nicht länger erreichbar, da die Testadressen während eines Failover ignoriert werden. Um sicherzustellen, dass das IP die Testadresse nicht für normale Anwendungen auswählt, markieren Sie die Testadresse als `deprecated` (eingestellt).

IPv4 verwendet keine eingestellte Adresse als Quelladresse einer Kommunikation, es sei denn, eine Anwendung ist explizit an die Adresse gebunden. Der `in.mpathd`-Daemon ist explizit an eine solche Adresse gebunden, um Stichprobenverkehr senden und empfangen zu können.

Da Link-lokale IPv6-Adressen in einem Namen-Service normalerweise nicht vorhanden sind, verwenden DNS- und NIS-Anwendungen keine Link-lokale Adressen zur Kommunikation. Entsprechend dürfen Sie Link-lokale IPv6-Adressen nicht als `deprecated` kennzeichnen.

IPv4-Testadressen dürfen nicht in die DNS-Namen-Servicetabellen eingefügt werden. Unter IPv6 werden Link-lokale Adressen im Allgemeinen nicht in die Namen-Servicetabellen eingefügt.

IPMP-Schnittstellenkonfigurationen

Eine IPMP-Konfiguration setzt sich in Allgemeinen aus mindestens zwei physikalischen Schnittstellen im gleichen System zusammen, die an den gleichen IP-Link angeschlossen sind. Diese physikalischen Schnittstellen können, müssen sich aber nicht auf der gleichen NIC befinden. Die Schnittstellen sind als Mitglieder der gleichen IPMP-Gruppe konfiguriert. Wenn das System über zusätzliche Schnittstellen auf einem zweiten IP-Link verfügt, müssen Sie diese Schnittstellen als eine weitere IPMP-Gruppe konfigurieren.

Eine einzelne Schnittstelle kann in ihrer eigenen IPMP-Gruppe konfiguriert werden. Eine IPMP-Gruppe mit nur einer Schnittstelle weist das gleiche Verhalten wie eine IPMP-Gruppe mit mehreren Schnittstellen auf. Failover und Failback können jedoch nur für eine IPMP-Gruppe mit mehreren Schnittstellen stattfinden.

Sie können VLANs auch mit dem gleichen Verfahren in eine IPMP-Gruppe konfigurieren, mit dem Sie auch eine Gruppe aus IP-Schnittstellen bilden. Die Vorgehensweisen finden Sie unter „Konfiguration von IPMP-Gruppen“ auf Seite 801. Die unter „Allgemeine Anforderungen von IPMP“ auf Seite 783 aufgeführten Vorausssetzungen gelten auch für die Konfiguration von VLANs in eine IPMP-Gruppe.

Achtung – Die zur Benennung von VLANs geltende Konvention kann zu Fehlern führen, wenn Sie VLANs als IPMP-Gruppe konfigurieren. Weitere Details zu VLAN-Namen finden Sie unter „VLAN-Tags und physikalischer Anschlusspunkt“ auf Seite 168 im *System Administration Guide: IP Services*. Betrachten wir ein Beispiel mit vier VLANs: `bge1000`, `bge1001`, `bge2000` und `bge2001`. Für eine IPMP-Implementierung müssen diese VLANs wie folgt gruppiert werden: `bge1000` und `bge1001` gehören zu einer Gruppe und zu VLAN 1, wohingegen `bge2000` und `bge2001` zu einer anderen Gruppe in VLAN 2 gehören. Aufgrund der VLAN-Namen kann es leicht zu Verwechslungen zwischen VLANs kommen, die unterschiedlichen Links in einer IPMP-Gruppe angehören, beispielsweise `bge1000` und `bge2000`.

Standby-Schnittstellen in einer IPMP-Gruppe

Die *Standby-Schnittstelle* in einer IPMP-Gruppe wird nicht für Datenverkehr verwendet, es sei denn, eine andere Schnittstelle in der Gruppe fällt aus. In diesem Fall migrieren die Datenadressen der ausgefallenen Schnittstelle zur Standby-Schnittstelle. Dann wird die Standby-Schnittstelle wie andere aktive Schnittstellen behandelt, bis die ausgefallene Schnittstelle repariert wurde. Manchmal wird bei einem Failover nicht die Standby-Schnittstelle sondern eine andere aktive Schnittstelle ausgewählt, für die weniger aktive Datenadressen als für die Standby-Schnittstelle konfiguriert sind.

Für eine Standby-Schnittstelle sollten nur Testadressen konfiguriert werden. IPMP gestattet es nicht, eine Datenadresse zu einer Schnittstelle hinzuzufügen, die mithilfe des Befehls `ifconfig` als `Standby`-Schnittstelle konfiguriert wurde. Jeder Versuch, diesen Konfigurationstyp zu

erstellen, schlägt fehl. Entsprechend gilt, wenn Sie eine Schnittstelle, die bereits über Datenadressen verfügt, als eine `Standby`-Schnittstelle konfigurieren, führen diese Adressen automatisch einen Failover auf eine andere Schnittstelle in der IPMP-Gruppe durch. Aufgrund dieser Einschränkungen müssen Sie den `ifconfig`-Befehl verwenden, um Testadressen als `deprecated` und `-failover` zu kennzeichnen, bevor die Schnittstelle als `Standby` eingerichtet wird. Informationen zur Konfiguration von Standby-Schnittstellen finden Sie unter „So konfigurieren Sie eine Standby-Schnittstelle für eine IPMP-Gruppe" auf Seite 808.

Allgemeine IPMP-Schnittstellenkonfigurationen

Wie bereits unter „IPMP-Adressierung" auf Seite 784 beschrieben, wickeln Schnittstellen in einer IPMP-Gruppe, abhängig von der Schnittstellenkonfiguration, normalen Datenverkehr und Stichprobenverkehr ab. Mit dem IPMP-Optionen des Befehls `ifconfig` können Sie eine entsprechende Konfiguration erstellen.

Eine *aktive Schnittstelle* ist eine physikalische Schnittstelle, die sowohl Datenverkehr als auch Stichprobenverkehr übermittelt. Die Konfiguration einer Schnittstelle als „aktive Schnittstelle" erfolgt mithilfe der Aufgabe „So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen" auf Seite 801 oder der Aufgabe „So konfigurieren Sie eine IPMP-Gruppe mit nur einer Schnittstelle" auf Seite 811.

im Folgenden sind zwei allgemeine IPMP-Konfigurationsarten beschrieben:

Aktiv-aktive Konfiguration Eine IPMP-Gruppe mit zwei Schnittstellen, die beide „aktiv" sind, d. h. sie übertragen zu jeder Zeit sowohl Stichprobendaten als auch den regulären Datenverkehr.

Aktiv-Standby-Konfiguration Eine IPMP-Gruppe mit zwei Schnittstellen, von denen eine als „Standby" konfiguriert ist."

Überprüfen des Status einer Schnittstelle

Mit dem Befehl `ifconfig` *Schnittstelle* können Sie den Status einer Schnittstelle überprüfen. Allgemeine Informationen zum Statusbericht des Befehls `ifconfig` finden Sie unter So zeigen Sie Informationen zu einer bestimmten Schnittstelle an.

Beispielsweise können Sie den Status einer Standby-Schnittstelle mit dem Befehl `ifconfig` abrufen. Wenn die Standby-Schnittstelle keine Datenadresse hostet, hat sie Flag `INACTIVE` für ihren Status gesetzt. Sie finden dieses Flag in den Statuszeilen der Schnittstelle in der Ausgabe des Befehls `ifconfig`.

IPMP-Funktionen zur Ausfall- und Reparaturerkennung

Der `in.mpathd`-Daemon kann die folgenden Arten einer Ausfallerkennung verarbeiten:

- Link-basierte Ausfallerkennung, sofern diese vom NIC-Treiber unterstützt wird
- Stichproben-basierte Ausfallerkennung, wenn Testadressen konfiguriert wurden
- Erkennung von Schnittstellen, die beim Booten nicht vorhanden sind

In der Manpage `in.mpathd`(1M) wird ausführlich beschrieben, wie der `in.mpathd`-Daemon die Erkennung von ausgefallenen Schnittstellen verarbeitet.

Stichproben-basierte Ausfallerkennung

Die Stichproben-basierte Ausfallerkennung ist immer aktiviert, vorausgesetzt, die Schnittstelle unterstützt diese Art der Ausfallerkennung. In der aktuellen Version von Oracle Solaris werden die folgenden Sun-Netzwerktreiber unterstützt:

- `hme`
- `eri`
- `ce`
- `ge`
- `bge`
- `qfe`
- `dmfe`
- `e1000g`
- `ixgb`
- `nge`
- `nxge`
- `rge`
- `xge`

Informationen, ob eine Schnittstelle eines Drittanbieters die Stichproben-basierte Ausfallerkennung unterstützt, entnehmen Sie bitte der Dokumentation des jeweiligen Herstellers.

Diese Netzwerk-Schnittstellentreiber überwachen den Verbindungsstatus einer Schnittstelle und benachrichtigen das Netzwerk-Untersystem, wenn sich der Verbindungsstatus ändert. Wenn das Netzwerk-Untersystem über eine Änderung informiert wird, setzt oder löscht es das Flag `RUNNING` für diese Schnittstelle. Erkennt der Daemon, dass das Flag `RUNNING` einer Schnittstelle gelöscht wurde, lässt er die Schnittstelle unverzüglich ausfallen.

Stichproben-basierte Ausfallerkennung

Der `in.mpathd`-Daemon führt für jede Schnittstelle in der IPMP-Gruppe, die über eine Testadresse verfügt, eine Stichproben-basierte Ausfallerkennung durch. Eine Stichproben-basierte Ausfallerkennung umfasst das Senden und Empfangen von ICMP-Stichprobennachrichten an bzw. von den Testadressen. Diese Nachrichten werden über die Schnittstelle an eines oder mehrere Zielsysteme auf dem gleichen IP-Link gesendet. Eine Einführung in das Konzept der Testadressen finden Sie unter „Testadressen“ auf Seite 784. Informationen zur Konfiguration von Testadressen finden Sie unter „So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen“ auf Seite 801.

Der `in.mpathd`-Daemon legt fest, an welche Zielsysteme dynamisch Stichproben gesendet werden. Router, die mit dem IP-Link verbunden sind, werden automatisch als Ziele für Stichproben ausgewählt. Falls keine Router auf dem Link vorhanden sind, sendet `in.mpathd` die Stichproben an die Nachbar-Hosts auf dem Link. Ein Multicast-Paket, das die Multicast-Adresse aller Hosts (`224.0.0.1` bei IPv4 und `ff02::1` bei IPv6) gesendet wird, legt fest, welche Hosts als Zielsysteme verwendet werden. Die ersten Hosts, die auf die Echo-Pakete antworten, werden als Ziele für die Stichproben ausgewählt. Wenn `in.mpathd` keine Router findet oder keine Hosts auf die ICMP-Echo-Pakete antworten, kann der `in.mpathd`-Daemon keine Ausfälle anhand von Stichproben erkennen.

Sie können Host-Routen verwenden, um explizit eine Liste mit Zielsystemen zu konfigurieren, die von `in.mpathd` verwendet werden sollen. Anweisungen hierzu finden Sie unter „Konfiguration von Zielsystemen“ auf Seite 806.

Um sicherzustellen, dass jede Schnittstelle in der IPMP-Gruppe ordnungsgemäß funktioniert, testet der `in.mpathd`-Daemon alle Ziele separat über alle Schnittstellen in der IPMP-Gruppe. Falls auf fünf aufeinander folgende Stichproben keine Antworten eingehen, betrachtet `in.mpathd` die Schnittstelle als ausgefallen. Die Stichprobenrate hängt von der *Failure Detection Time* (FDT) ab. Der Standardwert der Failure Detection Time beträgt 10 Sekunden. Sie können die Failure Detection Time jedoch in der Datei `/etc/default/mpathd` ändern. Anweisungen finden Sie in „So konfigurieren Sie die `/etc/default/mpathd`-Datei“ auf Seite 821.

Bei einer Reparatur-Erkennungszeit von 10 Sekunden beträgt die Stichprobenrate etwa eine Stichprobe alle 2 Sekunden. Die Reparatur-Erkennungszeit beträgt das Doppelte der Failure Detection Time (standardmäßig 20 Sekunden), da Antworten auf 10 aufeinander folgende Stichproben empfangen werden müssen. Die Ausfall- und Reparatur-Erkennungszeiten gelten nur für die Stichproben-basierte Ausfallerkennung.

Hinweis – In einer aus VLANs bestehenden IPMP-Gruppe wird die Link-basierte Fehlererkennung über physische Links implementiert und wirkt sich deswegen auf alle VLANs dieses Links aus. Die stichprobenbasierte Fehlererkennung wird pro VLAN-Link durchgeführt. So sind `bge0`/`bge1` und `bge1000`/`bge1001` beispielsweise zusammen in einer Gruppe konfiguriert. Wenn das Kabel für `bge0` herausgezogen wird, meldet die Link-basierte Fehlererkennung sowohl `bge0` als auch `bge1000` sofort als ausgefallen. Wenn jedoch alle Stichprobenziele auf `bge0` nicht erreichbar sind, wird nur `bge0` als ausgefallen gemeldet, da `bge1000` seine eigenen Stichprobenziele in seinem eigenen VLAN besitzt.

Ausfall einer Gruppe

Ein *Ausfall einer Gruppe* tritt auf, wenn alle Schnittstellen in einer IPMP-Gruppe scheinbar gleichzeitig ausfallen. Bei einem Ausfall einer Gruppe kann der `in.mpathd`-Daemon keinen Failover durchführen. Darüber hinaus findet kein Failover statt, wenn alle Zielsysteme gleichzeitig ausfallen. In diesem Fall löscht `in.mpathd` alle aktuellen Zielsysteme und beginnt mit der Erkennung neuer Zielsysteme.

Erkennen der Reparatur physikalischer Schnittstellen

Damit der `in.mpathd`-Daemon eine Schnittstelle als repariert ansehen kann, muss das Flag `RUNNING` für die Schnittstelle gesetzt sein. Wenn die Stichproben-basierte Ausfallerkennung verwendet wird, muss der `in.mpathd`-Daemon Antworten auf 10 aufeinander folgende Stichprobenpakete von der Schnittstelle empfangen. Erst dann wird die Schnittstelle als repariert angesehen. Anschließend wandern alle Adressen, für die ein Failover auf eine andere Schnittstelle stattgefunden hat, zur reparierten Schnittstelle zurück (Failback). Wurde eine Schnittstelle vor dem Ausfall als „aktiv" konfiguriert, kann die Schnittstelle nach der Reparatur das Senden und Empfangen von Verkehr wieder aufnehmen.

Vorgänge während eines Schnittstellen-Failover

In den folgenden zwei Beispielen wird eine typische Konfiguration gezeigt und wie sich diese Konfiguration automatisch ändert, wenn eine Schnittstelle ausfällt. Wenn die Schnittstelle `hme0` ausfällt, achten Sie darauf, wie alle Datenadressen von `hme0` zu `hme1` geändert werden.

BEISPIEL 30–1 Schnittstellenkonfiguration vor dem Ausfall einer Schnittstelle

```
hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
     mtu 1500 index 2
     inet 192.168.85.19 netmask ffffff00 broadcast 192.168.85.255
     groupname test
hme0:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
```

BEISPIEL 30–1 Schnittstellenkonfiguration vor dem Ausfall einer Schnittstelle *(Fortsetzung)*

```
     mtu 1500
     index 2 inet 192.168.85.21 netmask ffffff00 broadcast 192.168.85.255
hme1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
8     inet 192.168.85.20 netmask ffffff00 broadcast 192.168.85.255
     groupname test
hme1:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
     mtu 1500
     index 2 inet 192.168.85.22 netmask ffffff00 broadcast 192.168.85.255
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
     inet6 fe80::a00:20ff:feb9:19fa/10
     groupname test
hme1: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
     inet6 fe80::a00:20ff:feb9:1bfc/10
     groupname test
```

BEISPIEL 30–2 Schnittstellenkonfiguration nach dem Ausfall einer Schnittstelle

```
hme0: flags=19000842<BROADCAST,RUNNING,MULTICAST,IPv4,
      NOFAILOVER,FAILED> mtu 0 index 2
      inet 0.0.0.0 netmask 0
      groupname test
hme0:1: flags=19040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,
      NOFAILOVER,FAILED> mtu 1500 index 2
      inet 192.168.85.21 netmask ffffff00 broadcast 10.0.0.255
hme1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 192.168.85.20 netmask ffffff00 broadcast 192.168.85.255
      groupname test
hme1:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,
      NOFAILOVER> mtu 1500
      index 2 inet 192.168.85.22 netmask ffffff00 broadcast 10.0.0.255
hme1:2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 6
      inet 192.168.85.19 netmask ffffff00 broadcast 192.168.18.255
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER,FAILED> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:19fa/10
      groupname test
hme1: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:1bfc/10
      groupname test
```

Sie sehen, dass das Flag `FAILED` für die Schnittstelle `hme0` gesetzt ist, um zu kennzeichnen, dass diese Schnittstelle ausgefallen ist. Sie sehen auch, dass `hme1:2` erstellt wurde. `hme1:2` war ursprünglich `hme0`. Die Adresse `192.168.85.19` wurde daraufhin über `hme1` zugänglich.

Multicast-Mitgliedschaften, die `192.168.85.19` zugeordnet sind, können noch immer Pakete empfangen, jetzt jedoch über `hme1`. Nachdem der Failover der Adresse `192.168.85.19` von `hme0` auf `hme1` stattgefunden hat, wurde eine Dummy-Adresse `0.0.0.0` auf `hme0` erstellt. Die Dummy-Adresse wurde so erstellt, dass weiterhin auf `hme0` zugegriffen werden kann. `hme0:1` kann nicht ohne `hme0` existieren. Die Dummy-Adresse wurde wieder entfernt, nachdem letztlich ein Failback stattgefunden hat.

Entsprechend fand ein Failover der IPv6-Adresse von hme0 zu hme1 statt. Bei IPv6 sind Multicast-Mitgliedschaften den Schnittstellenindexen zugeordnet. Auch für Multicast-Mitgliedschaften findet ein Failover von hme0 zu hme1 statt. Alle von in.ndpd konfigurierten Adressen werden ebenfalls verschoben. Diese Aktion wird in den Beispielen jedoch nicht gezeigt.

Der in.mpathd-Daemon sendet weiterhin Stichproben über die ausgefallene Schnittstelle hme0. Nachdem der Daemon 10 aufeinander folgende Antworten über die Standard-Reparaturerkennungszeit von 20 Sekunden empfangen hat, betrachtet der Daemon die Schnittstelle als repariert. Da auch das Flag RUNNING für die Schnittstelle hme0 gesetzt ist, ruft der Daemon den Failback-Prozess auf. Nach dem Failback wird die ursprüngliche Konfiguration wieder hergestellt.

Eine Beschreibung aller Fehlermeldungen, die während des Ausfalls und den Reparaturen auf der Konsole protokolliert wurden, finden Sie in der Manpage in.mpathd(1M).

IPMP und Dynamische Rekonfiguration

Mit der dynamischen Rekonfiguration (DR) können Sie bei laufendem System Systemhardware wie z. B. Schnittstellen neu konfigurieren. In diesem Abschnitt wird beschrieben, wie DR mit IPMP zusammenarbeitet.

Bei einem System, das die DR von NICs unterstützt, kann IPMP dazu beitragen, die Konnektivität aufrecht zu erhalten und eine Unterbrechung von bestehenden Verbindungen zu verhindern. Auf einem System, das DR unterstützt und IPMP verwendet, können Sie NICs problemlos anschließen, trennen oder erneut anschließen, denn IPMP ist in das Reconfiguration Coordination Manager (RCM)-Framework integriert. *RCM* verwaltet die dynamische Rekonfiguration von Systemkomponenten.

Normalerweise verwenden Sie den Befehl cfgadm zum Ausführen von DR-Vorgängen. Einige Plattformen unterstützen jedoch auch andere Methoden. Einzelheiten finden Sie in der Dokumentation Ihrer Plattform. Dokumentationen zur DR finden Sie in den folgenden Ressourcen.

TABELLE 30–1 Dokumentationen zur dynamischen Rekonfiguration

Beschreibung	Weitere Informationen
Ausführliche Informationen zum Befehl cfgadm	Manpage cfgadm(1M)
Spezifische Informationen zur DR in der Sun Cluster-Umgebung	*Sun Cluster 3.1 System Administration Guide*
Spezifische Informationen zur DR in der Sun Fire-Umgebung	*Sun Fire 880 Dynamic Reconfiguration Guide*

TABELLE 30–1 Dokumentationen zur dynamischen Rekonfiguration *(Fortsetzung)*

Beschreibung	Weitere Informationen
Einführung in die DR und den Befehl `cfgadm`	Kapitel 6, „Dynamically Configuring Devices (Tasks)" in *System Administration Guide: Devices and File Systems*
Aufgaben zur Verwaltung von IPMP-Gruppen auf einem System, das DR unterstützt	„Ersetzen einer ausgefallenen physikalischen Schnittstelle auf Systemen, die DR unterstützen" auf Seite 815

Anschließen von NICs

Mit dem Befehl `ifconfig` können Sie einer IPMP-Gruppe jederzeit Schnittstellen hinzufügen. Dies wird ausführlich unter „So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen" auf Seite 801 beschrieben. Somit können alle Schnittstellen auf Systemkomponenten, die nach dem Systemstart angeschlossen wurde, geplumbt und zu einer bestehenden IPMP-Gruppe hinzugefügt werden. Gegebenenfalls können Sie neu hinzugefügte Schnittstellen auch in einer eigenen IPMP-Gruppe konfigurieren.

Diese Schnittstellen und die darauf konfigurierten Datenadresse stehen unmittelbar für die Verwendung durch die IPMP-Gruppe zur Verfügung. Sie müssen jedoch eine `/etc/hostname.`*Schnittstelle*-Datei für jede neue Schnittstelle erstellen, damit das System diese Schnittstellen nach einem Neustart automatisch konfiguriert und verwendet. Anweisungen hierzu finden Sie unter So konfigurieren Sie eine physikalische Schnittstelle nach der Systeminstallation.

Falls diese `/etc/hostname.`*Schnittstelle*-Datei schon beim Anschließen der Schnittstelle vorhanden ist, konfiguriert RCM die Schnittstelle automatisch gemäß dem Inhalt dieser Datei. Somit erhält die Schnittstelle die gleiche Konfiguration, die sie nach einem Systemstart erhalten würde.

Trennen von NICs

Alle Anforderungen zum Trennen von Systemkomponenten mit NICs werden zunächst daraufhin geprüft, ob die Konnektivität aufrechterhalten werden kann. Beispielsweise können Sie standardmäßig keine NIC trennen, die sich nicht in einer IPMP-Gruppe befindet. Außerdem können Sie keine NIC trennen, die die einzigen ordnungsgemäß arbeitenden Schnittstellen in einer IPMP-Gruppe enthält. Wenn Sie die Systemkomponente entfernen müssen, können Sie dieses Verhalten jedoch mit der Option `-f` des Befehls `cfgadm` außer Kraft setzen. Lesen Sie dazu die Manpage `cfgadm`(1M).

Wenn die Prüfungen erfolgreich abgeschlossen wurden, führen die Datenadressen, die der zu trennenden NIC zugeordnet sind, einen Failover zu einer ordnungsgemäß arbeitenden NIC in der gleichen Gruppe aus, als ob die zu trennende NIC ausgefallen wäre. Nachdem die NIC

getrennt wurde, sind alle Testadressen der Schnittstellen auf der NIC in einem dekonfigurierten Zustand. Erst dann kann das Plumbing der NIC rückgängig gemacht werden. Wenn einer dieser Schritte fehlschlägt, oder wenn die DR einer anderen Hardware auf der gleichen Systemkomponente ausfällt, wird die vorherige Konfiguration im ursprünglichen Zustand wiederhergestellt. In diesem Fall erhalten Sie jedoch eine Statusnachricht. Andernfalls wird die Aufforderung zum Trennen erfolgreich abgeschlossen. Sie können die Komponente vom System entfernen. Bestehende Verbindungen werden nicht unterbrochen.

Wiederanschließen von NICs

RCM zeichnet die Konfigurationsinformationen von NICs auf, die von einem laufenden System getrennt wurden. Daher behandelt RCM das Wiederanschließen einer NIC, die zuvor getrennt wurde, genauso, als ob eine neue NIC angeschlossen wird. Das heißt, RCM führt lediglich das Plumbing der Schnittstelle durch.

Für wieder angeschlossene NICs existiert·jedoch in der Regel eine `/etc/hostname.`*Schnittstelle*-Datei. In diesem Fall konfiguriert RCM die Schnittstelle automatisch gemäß dem Inhalt der vorhandenen `/etc/hostname.` *Schnittstelle*-Datei. Zusätzlich informiert RCM den `in.mpathd`-Daemon über jede Datenadresse, die ursprünglich auf der wieder angeschlossenen Schnittstelle gehostet wurde. Das heißt, nachdem die wieder angeschlossene Schnittstelle ordnungsgemäß funktioniert, führen alle Datenadressen ein Failback auf die wieder angeschlossene Schnittstelle aus, als wäre sie repariert worden.

Verfügt die wieder angeschlossene NIC nicht über eine `/etc/hostname.`*Schnittstelle*-Datei, stehen keine Konfigurationsinformationen zur Verfügung. In diesem Fall hat RCM keine Informationen, wie die Schnittstelle konfiguriert werden soll. Adressen, die zuvor ein Failover zu einer anderen Schnittstelle durchgeführt haben, führen kein Failback durch.

Bei einem Systemstart fehlende NICs

NICs, die bei einem Systemstart nicht vorhanden sind, stellen einen Sonderfall bei der Ausfallerkennung dar. Beim Booten verfolgen die Startskripten alle Schnittstellen mit `/etc/hostname.`*Schnittstelle*-Dateien, für die kein Plumbing stattgefunden hat. Alle Datenadressen in der `/etc/hostname.` *Schnittstelle*-Datei einer solchen Schnittstelle werden automatisch unter einer alternativen Schnittstelle in der IPMP-Gruppe gehostet.

In diesem Fall erhalten Sie Fehlermeldungen ähnlich der Folgenden:

```
moving addresses from failed IPv4 interfaces: hme0 (moved to hme1)
moving addresses from failed IPv6 interfaces: hme0 (moved to hme1)
```

Falls keine alternative Schnittstelle vorhanden ist, erhalten Sie eine Fehlermeldung ähnlich der Folgenden:

```
moving addresses from failed IPv4 interfaces: hme0 (couldn't move;
   no alternative interface)
 moving addresses from failed IPv6 interfaces: hme0 (couldn't move;
   no alternative interface)
```

Hinweis – Bei dieser Ausfallerkennung wandern nur die Datenadressen, die explizit in der `/etc/hostname.`*Schnittstelle*-Datei aufgelistet sind, zu einer alternativen Schnittstelle. Alle Adressen, die normalerweise über andere Mittel, z. B. RARP oder DHCP erworben wurden, werden nicht übernommen oder verschoben.

Wenn eine Schnittstelle mit den gleichen Namen wie eine beim Booten des Systems fehlende Schnittstellt mit DR wieder angeschlossen wird, führt RCM das Plumbing der Schnittstelle durch. Dann konfiguriert RCM die Schnittstelle gemäß dem Inhalt der zugehörigen `/etc/hostname.`*Schnittstelle*-Datei. Schließlich führt RCM ein Failback aller Datenadressen durch, als ob die Schnittstelle repariert wurde. Somit ist die endgültige Netzwerkkonfiguration identisch mit der Konfiguration, die übernommen worden wäre, wenn das System mit vorhandener Schnittstelle gebootet wäre.

KAPITEL 31

Verwaltung von IPMP (Aufgaben)

In diesem Kapitel sind die Aufgaben zur Verwaltung von Schnittstellengruppen mit IP Network Multipathing (IPMP) beschrieben. Folgende Themen werden behandelt:

- „Konfiguration von IPMP (Übersicht der Schritte)“ auf Seite 797
- „Konfiguration von IPMP-Gruppen“ auf Seite 799
- „Verwalten von IPMP-Gruppen“ auf Seite 812
- „Ersetzen einer ausgefallenen physikalischen Schnittstelle auf Systemen, die DR unterstützen“ auf Seite 815
- „Wiederherstellung einer physikalischen Schnittstelle, die beim Systemstart nicht vorhanden war“ auf Seite 818
- „Ändern von IPMP-Konfigurationen“ auf Seite 820

Eine Einführung in das IPMP-Konzept finden Sie in Kapitel 30, „Einführung in IPMP (Übersicht)“.

Konfiguration von IPMP (Übersicht der Schritte)

Dieser Abschnitt enthält Links zu den in diesem Kapitel beschriebenen Aufgaben.

Konfiguration und Verwaltung von IPMP-Gruppen (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Planung für eine IPMP-Gruppe.	Erstellen Sie eine Liste aller Zusatzinformationen und erforderlichen Aufgaben, bevor Sie mit der Konfiguration einer IPMP-Gruppe beginnen.	„So planen Sie für eine IPMP-Gruppe“ auf Seite 799
Konfiguration einer IPMP-Schnittstellengruppe mit mehreren Schnittstellen.	Konfigurieren Sie mehrere Schnittstellen als Mitglieder einer IPMP-Gruppe.	„So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen“ auf Seite 801
Konfiguration einer IPMP-Gruppe, in der eine Schnittstelle als Standby-Schnittstelle fungiert.	Konfigurieren Sie eine der Schnittstellen in einer IPMP-Gruppe mit mehreren Schnittstellen als eine Standby-Schnittstelle.	„So konfigurieren Sie eine Standby-Schnittstelle für eine IPMP-Gruppe“ auf Seite 808
Konfiguration einer IPMP-Gruppe, die aus nur einer Schnittstelle besteht.	Erstellen Sie eine IPMP-Gruppe mit nur einer Schnittstelle.	„So konfigurieren Sie eine IPMP-Gruppe mit nur einer Schnittstelle“ auf Seite 811
Anzeigen der IPMP-Gruppe, zu der eine physikalische Schnittstelle gehört.	Beziehen Sie den Namen der IPMP-Gruppe einer Schnittstelle aus der Ausgabe des Befehls `ifconfig`.	„So zeigen Sie die IPMP-Gruppenmitgliedschaft einer Schnittstelle an“ auf Seite 812
Hinzufügen einer Schnittstelle zu einer IPMP-Gruppe.	Konfigurieren Sie eine neue Schnittstelle als ein Mitglied einer bestehenden IPMP-Gruppe.	„So fügen Sie eine Schnittstelle zu einer IPMP-Gruppe hinzu“ auf Seite 813
Entfernen einer Schnittstelle aus einer IPMP-Gruppe.	Entfernen Sie eine Schnittstelle aus einer IPMP-Gruppe.	„So entfernen Sie eine Schnittstelle aus einer IPMP-Gruppe“ auf Seite 814
Verschieben einer Schnittstelle aus einer vorhandenen IPMP-Gruppe in eine andere Gruppe.	Verschieben Sie Schnittstellen zwischen IPMP-Gruppen.	„So verschieben Sie eine Schnittstelle von einer IPMP-Gruppe in eine andere“ auf Seite 815
Ändern von drei Standardeinstellungen für den `in.mpathd`-Daemon.	Ändern Sie die Failure Detection Time sowie andere Parameter des `in.mpathd`-Daemons.	„So konfigurieren Sie die `/etc/default/mpathd`-Datei“ auf Seite 821

Verwalten von IPMP auf Schnittstellen, die DR unterstützen (Übersicht der Schritte)

Aufgabe	Beschreibung	Siehe
Entfernen einer ausgefallenen Schnittstelle.	Entfernen Sie eine ausgefallene Schnittstelle von einem System.	„So entfernen Sie eine ausgefallene physikalische Schnittstelle (DR-Detach)“ auf Seite 816
Ersetzen einer ausgefallenen Schnittstelle.	Ersetzen Sie eine ausgefallene Schnittstelle.	„So ersetzen Sie eine ausgefallene physikalische Schnittstelle (DR-Attach)“ auf Seite 817
Wiederherstellen einer Schnittstelle, die beim Booten nicht konfiguriert wurde.	Stellen Sie eine ausgefallene Schnittstelle wieder her.	„So stellen Sie eine physikalische Schnittstelle wieder her, die beim Systemstart nicht vorhanden war“ auf Seite 818

Konfiguration von IPMP-Gruppen

In diesem Abschnitt finden Sie Verfahren zur Konfiguration von IPMP-Gruppen. Darüber hinaus wird hier beschrieben, wie eine Schnittstelle als Standby-Schnittstelle konfiguriert wird.

Planung für eine IPMP-Gruppe

Bevor Sie die Schnittstellen eines Systems als Teil einer IPMP-Gruppe konfigurieren können, müssen Sie einige Planungsaufgaben durchführen.

▼ So planen Sie für eine IPMP-Gruppe

Im folgenden Verfahren werden Aufgaben zur Planung und Informationen beschrieben, die vor der Konfiguration einer IPMP-Gruppe zusammengetragen werden müssen. Die Aufgaben müssen nicht in der angegebenen Reihenfolge ausgeführt werden.

1. **Entscheiden Sie, welche Schnittstellen auf dem System Teil der IPMP-Gruppe werden sollen.**

   Eine IPMP-Gruppe besteht in der Regel aus mindestens zwei physikalischen Schnittstellen, die an den gleichen IP-Link angeschlossen sind. Falls erforderlich, können Sie auch eine IPMP-Gruppe mit nur einer Schnittstelle konfigurieren. Eine Einführung in IPMP-Gruppen finden Sie unter „IPMP-Schnittstellenkonfigurationen“ auf Seite 787. Beispielsweise können Sie den gleichen Ethernet-Switch oder das gleiche IP-Teilnetz unter der gleichen IPMP-Gruppe konfigurieren. Sie können beliebig viele Schnittstellen in der gleichen IPMP-Gruppe konfigurieren.

Der Parameter `group` des Befehls `ifconfig` kann nicht mit logischen Schnittstellen verwendet werden. Entsprechend können Sie den Parameter `group` mit `hme0`, aber nicht mit `hme0:1` verwenden.

2 Prüfen Sie, ob jede Schnittstelle in der Gruppe über eine einmalige MAC-Adresse verfügt.

Anweisungen hierzu finden Sie unter „SPARC: So stellen Sie sicher, dass die MAC-Adresse einer Schnittstelle einmalig ist“ auf Seite 163.

3 Wählen Sie einen Namen für die IPMP-Gruppe.

Es kann jeder Name außer Null kann für die Gruppe verwendet werden. Sie sollten einen Namen verwenden, der den IP-Link beschreibt, an den die Schnittstellen angeschlossen sind.

4 Achten Sie darauf, dass der gleiche Satz `STREAMS`-Module auf alle Schnittstellen in der IPMP-Gruppe gepusht und konfiguriert wird.

Auf allen Schnittstellen in einer Gruppe müssen die gleichen `STREAMS`-Module in der gleichen Reihenfolge konfiguriert werden.

a. Überprüfen Sie an allen Schnittstellen in der künftigen IPMP-Gruppe die Reihenfolge der STREAMS-Module.

Mit dem Befehl `ifconfig` *Schnittstelle* `modlist` drucken Sie eine Liste der `STREAMS`-Module. Das Folgende ist die Ausgabe des Befehls `ifconfig` für die Schnittstelle `hme0`:

```
# ifconfig hme0 modlist
    0 arp
    1 ip
    2 hme
```

Schnittstellen existieren normalerweise als Netzwerktreiber direkt unterhalb des IP-Moduls. Diese wird in der Ausgabe von `ifconfig hme0 modlist` gezeigt. Sie sollten keine zusätzliche Konfiguration erfordern.

Einige Technologien, z. B. NCA oder IP Filter, fügen sich jedoch selbst als STREAMS-Module zwischen dem IP-Modul und dem Netzwerktreiber ein. Dabei können Probleme durch das Verhalten der Schnittstellen in der gleichen IPMP-Gruppe entstehen.

Ist ein STREAMS-Modul statusbehaftet, kann bei einem Failover ein unerwartetes Verhalten auftreten. Dies erfolgt unabhängig davon, ob Sie das gleiche Modul auf alle Schnittstellen in einer Gruppe pushen. Sie können jedoch statusfreie STREAMS-Module verwenden, vorausgesetzt, Sie pushen auf allen Schnittstellen in der IPMP-Gruppe in der gleichen Reihenfolge.

b. Pushen Sie die Module einer Schnittstelle in der Standardreihenfolge für die IPMP-Gruppe.

`ifconfig` *interface* **`modinsert`** *module-name*

```
ifconfig hme0 modinsert ip
```

5 Verwenden Sie für alle Schnittstellen der IPMP-Gruppe das gleiche IP-Adressierungsformat.

Wenn eine dieser Schnittstellen für IPv4 konfiguriert ist, müssen alle Schnittstellen der Gruppe für IPv4 konfiguriert sein. Angenommen, es besteht eine IPMP-Gruppe, die aus Schnittstellen von mehreren NICs zusammengesetzt ist. Wenn Sie zu den Schnittstellen einer Netzwerkkarte IPv6-Adressierung hinzufügen, müssen alle Schnittstelle in der IPMP-Gruppe so konfiguriert werden, dass sie IPv6 unterstützen.

6 Überprüfen Sie, ob alle Schnittstellen in der IPMP-Gruppe an den gleichen IP-Link angeschlossen sind.

7 Stellen Sie sicher, dass die IPMP-Gruppe keine Schnittstellen unterschiedlicher Netzwerkmedientypen enthält.

Die gruppierten Schnittstellen müssen den gleichen Schnittstellentyp gemäß Definition in `/usr/include/net/if_types.h` aufweisen. Beispielsweise können Sie Ethernet- und Token Ring-Schnittstellen nicht in einer IPMP-Gruppe kombinieren. Ein anderes Beispiel: Sie können eine Token Bus-Schnittstelle nicht mit Asynchronous Transfer Mode (ATM)-Schnittstellen in der gleichen IPMP-Gruppe kombinieren.

8 Bei IPMP mit ATM-Schnittstellen konfigurieren Sie die ATM-Schnittstellen im LAN-Emulationsmodus.

IPMP wird für Schnittstellen, die klassisches IP über ATM verwenden, nicht unterstützt.

Konfiguration von IPMP-Gruppen

Dieser Abschnitt enthält Aufgaben zur Konfiguration einer typischen IPMP-Gruppe mit mindestens zwei physikalischen Schnittstellen.

- Eine Einführung in IPMP-Gruppen mit mehreren Schnittstellen finden Sie unter „IPMP-Gruppe“ auf Seite 782.
- Aufgaben zur Planung finden Sie unter „Planung für eine IPMP-Gruppe“ auf Seite 799.
- Informationen zur Konfiguration einer IPMP-Gruppe mit nur einer physikalischen Schnittstelle finden Sie unter „Konfiguration von IPMP-Gruppen mit einer physikalischen Schnittstelle“ auf Seite 810.

▼ So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen

Die folgenden Schritte zum Konfigurieren einer IPMP-Gruppe gelten auch beim Konfigurieren von VLANs in einer IPMP-Gruppe.

Bevor Sie beginnen Sie müssen die IPv4-Adressen und, falls zutreffend, die IPv6-Adressen aller Schnittstellen in der geplanten IPMP-Gruppe vorab konfigurieren.

Achtung – Sie müssen für jedes Teilnetz oder jede L2-Broadcast-Domäne nur eine IPMP-Gruppe konfigurieren. Weitere Informationen finden Sie unter „Allgemeine Anforderungen von IPMP“ auf Seite 783

1. **Nehmen Sie auf dem System mit den zu konfigurierenden Schnittstellen die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Fügen Sie jede physikalische Schnittstelle einer IPMP-Gruppe hinzu.**

   `# ifconfig` *interface* `group` *group-name*

   Um beispielsweise `hme0` und `hme1` in die Gruppe `testgroup1` einzufügen, geben Sie die folgenden Befehle ein:

   ```
   # ifconfig hme0 group testgroup1
   # ifconfig hme1 group testgroup1
   ```

   Vermeiden Sie Leerzeichen in Gruppennamen. Der `ifconfig`-Status zeigt keine Leerzeichen an. Entsprechend dürfen Sie keine zwei ähnlichen Gruppennamen erstellen, deren einziger Unterschied darin besteht, dass einer der Gruppennamen ein Leerzeichen enthält. In diesem Fall sehen diese Gruppennamen in der Statusanzeige gleich aus.

   In einer Dual-Stack-Umgebung wird durch das Hinzufügen der IPv4-Instanz einer Schnittstelle in einer bestimmten Gruppe automatisch die IPv6-Instanz der gleichen Gruppe hinzugefügt.

3. **(Optional) Konfigurieren Sie eine IPv4-Testadresse auf einer oder mehreren physikalischen Schnittstellen.**

   Sie müssen nur dann eine Testadresse konfigurieren, wenn Sie die Stichproben-basierte Ausfallerkennung für eine bestimmte Schnittstelle verwenden. Testadressen werden als logische Schnittstellen der physikalischen Schnittstellen konfiguriert, die Sie für den Befehl `ifconfig` angegeben haben.

   Wenn eine Schnittstelle in der Gruppe als Standby-Schnittstelle konfiguriert werden soll, darf zu diesem Zeitpunkt keine Testadresse für die Schnittstelle konfiguriert werden. Die Konfiguration einer Testadresse für die Standby-Schnittstelle erfolgt im Rahmen der Aufgabe „So konfigurieren Sie eine Standby-Schnittstelle für eine IPMP-Gruppe“ auf Seite 808.

   Zur Konfiguration einer Testadresse verwenden Sie die folgende Syntax des Befehls `ifconfig`:

   `# ifconfig` *interface* `addif` *ip-address parameters* `-failover deprecated up`

Angenommen, Sie erstellen die folgende Testadresse für die primäre Netzwerkschnittstelle `hme0`:

```
# ifconfig hme0 addif 192.168.85.21 netmask + broadcast + -failover deprecated up
```

Dieser Befehl richtet die folgenden Parameter für die primäre Netzwerkschnittstelle `hme0` ein:

- Die Adresse wird auf `192.168.85.21` gesetzt
- Netzmasken- und Broadcast-Adresse werden auf den Standardwert gesetzt
- `-Failover`- und `deprecated`-Optionen werden gesetzt

Hinweis – Sie müssen eine IPv4-Testadresse als `deprecated` kennzeichnen, um zu verhindern, das diese Testadresse von Anwendungen verwendet wird.

---

4 Prüfen Sie die IPv4-Konfiguration einer bestimmten Schnittstelle.

Mit dem Befehl `ifconfig` *Schnittstelle* können Sie jederzeit den aktuellen Status einer Schnittstelle anzeigen. Weitere Informationen zum Anzeigen eines Schnittstellenstatus finden Sie unter So zeigen Sie Informationen zu einer bestimmten Schnittstelle an.

Sie erhalten Informationen zur Testadressenkonfiguration einer physikalischen Schnittstelle, indem Sie die logische Schnittstelle angeben, die der Testadresse zugewiesen ist.

```
# ifconfig hme0:1
    hme0:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
    mtu 1500 index 2
    inet 192.168.85.21 netmask ffffff00 broadcast 192.168.85.255
```

5 (Optional) Konfigurieren Sie bei Bedarf eine IPv6-Testadresse.

```
# ifconfig interface inet6 -failover
```

Physikalische Schnittstellen mit IPv6-Adressen werden in die gleichen IPMP-Gruppe wie die IPv4-Adressen der Schnittstellen eingefügt. Dies geschieht, wenn Sie die physikalische Schnittstelle mit IPv4-Adressen in einer IPMP-Gruppe konfigurieren. Wenn Sie zuerst physikalische Schnittstellen mit IPv6-Adressen in eine IPMP-Gruppe einfügen, werden die physikalischen Schnittstellen mit IPv4-Adressen ebenfalls implizit in die gleiche IPMP-Gruppe eingefügt.

Wenn Sie z. B. `hme0` mit einer IPv6-Testadresse konfigurieren, geben Sie Folgendes ein:

```
# ifconfig hme0 inet6 -failover
```

Sie müssen eine IPv6-Testadresse nicht als „deprecated“ kennzeichnen, um zu verhindern, dass diese Testadresse von Anwendungen verwendet wird.

6 Prüfen Sie die IPv6-Konfiguration.

```
# ifconfig hme0 inet6
    hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
```

```
inet6 fe80::a00:20ff:feb9:17fa/10
groupname test
```

Die IPv6-Testadresse ist die Link-lokale Adresse der Schnittstelle.

7 **(Optional) Behalten Sie die Konfiguration der IPMP-Gruppe nach einem Neustart bei.**

- Bei IPv4 fügen Sie die folgende Zeile zur `/etc/hostname.`*Schnittstelle*-Datei hinzu:

  ```
  interface-address <parameters> group group-name up \
      addif logical-interface -failover deprecated <parameters> up
  ```

  In diesem Fall wird die IPv4-Testadresse erst mit dem nächsten Neustart konfiguriert. Wenn die Konfiguration für die aktuelle Sitzung gelten soll, führen Sie die Schritte 1, 2 und optional 3 aus.

- Bei IPv6 fügen Sie die folgende Zeile zur `/etc/hostname6.` *Schnittstelle*-Datei hinzu:

  ```
  -failover group group-name up
  ```

  Diese IPv6-Testadresse wird erst mit dem nächsten Neustart konfiguriert. Wenn die Konfiguration für die aktuelle Sitzung gelten soll, führen Sie die Schritte 1, 2 und optional 5 aus.

8 **(Optional) Fügen Sie weitere Schnittstellen zur IPMP-Gruppe hinzu, indem Sie die Schritte 1 bis 6 wiederholen.**

Sie können bei einem laufenden System neue Schnittstellen zu einer vorhandenen Gruppe hinzufügen. Diese Änderungen gehen jedoch nach einem Neustart verloren.

Beispiel 31–1 Konfiguration einer IPMP-Gruppe mit zwei Schnittstellen

Angenommen, Sie möchten Folgendes umsetzen:

- Netzmasken- und Broadcast-Adresse sollen auf den Standardwert zurückgesetzt werden
- Die Schnittstelle soll mit der Testadresse `192.168.85.21` konfiguriert werden

Dazu geben Sie den folgenden Befehl ein:

```
# ifconfig hme0 addif 192.168.85.21 netmask + broadcast + -failover deprecated up
```

Sie müssen eine IPv4-Testadresse als `deprecated` kennzeichnen, um zu verhindern, das diese Testadresse von Anwendungen verwendet wird. Lesen Sie dazu „So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen“ auf Seite 801.

Um das Failover-Attribut der Adresse zu aktivieren, verwenden Sie die Option `failover` ohne das Minuszeichen.

Alle Testadressen in einer IPMP-Gruppe müssen das gleiche Netzwerkpräfix verwenden. Die IP-Testadressen müssen zum gleichen IP-Teilnetz gehören.

Beispiel 31–2 Beibehalten der Konfiguration einer IPv4-IPMP-Gruppe nach einem Neustart

Angenommen, Sie möchten eine IPMP-Gruppe namens `testgroup1` mit der folgenden Konfiguration erstellen:

- Physikalische Schnittstelle `hme0` mit der Datenadresse `192.168.85.19`
- Logische Schnittstelle mit der Testadresse `192.168.85.21`

Hinweis – In diesem Beispiel sind physikalische Schnittstelle und Datenadresse als Paar angeordnet. Gleiches gilt für die logische Schnittstelle und die Testadresse. Es existieren jedoch keine geerbten Beziehungen zwischen dem Schnittstellentyp und dem Adresstyp.

- `deprecated`- und `-failover`-Optionen sind gesetzt
- Netzmasken- und Broadcast-Adresse werden auf den Standardwert gesetzt

Sie fügen die folgende Zeile zur `/etc/hostname.hme0`-Datei hinzu:

```
192.168.85.19 netmask + broadcast + group testgroup1 up \
    addif 192.168.85.21 deprecated -failover netmask + broadcast + up
```

Entsprechend fügen Sie die folgende Zeile hinzu, um die zweite Schnittstelle `hme1` in der gleichen Gruppe `testgroup1` einzufügen und eine Testadresse zu konfigurieren:

```
192.168.85.20 netmask + broadcast + group testgroup1 up \
    addif 192.168.85.22 deprecated -failover netmask + broadcast + up
```

Beispiel 31–3 Beibehalten der Konfiguration einer IPv6 IPMP-Gruppe nach einem Neustart

Um eine Testgruppe für die Schnittstelle `hme0` mit einer IPv6-Adresse zu konfigurieren, fügen Sie die folgende Zeile zur `/etc/hostname6.hme0`-Datei hinzu:

```
-failover group testgroup1 up
```

Entsprechend fügen Sie die folgende Zeile zur `/etc/hostname6.hme1`-Datei hinzu, um die zweite Schnittstelle `hme1` in die Gruppe `testgroup1` einzufügen und eigene Testadresse zu konfigurieren:

```
-failover group testgroup1 up
```

Allgemeine Fehler Während der Konfiguration einer IPMP-Gruppe gibt `in.mpathd` zahlreiche Meldungen an die Systemkonsole oder in die Datei `syslog` aus. Diese Meldungen dienen nur zur Information und geben an, dass die IPMP-Konfiguration ordnungsgemäß funktioniert.

- Die folgende Meldung kennzeichnet, dass die Schnittstelle `hme0` zur IPMP-Gruppe `testgroup1` hinzugefügt wurde. Für `hme0` ist jedoch keine Testadresse konfiguriert. Um die Stichproben-basierte Ausfallerkennung zu aktivieren, müssen Sie der Schnittstelle eine Testadresse zuweisen.

  ```
  May 24 14:09:57 host1 in.mpathd[101180]:
  No test address configured on interface hme0;
  disabling probe-based failure detection on it.
  testgroup1
  ```
- Die folgende Meldung wird für alle Schnittstellen mit ausschließlich IPv4-Adressen angezeigt, die einer IPMP-Gruppe hinzugefügt wurden.

  ```
  May 24 14:10:42 host4 in.mpathd[101180]:
  NIC qfe0 of group testgroup1 is not
  plumbed for IPv6 and may affect failover capability
  ```
- Die folgende Nachricht wird angezeigt, wenn Sie eine Testadresse für eine Schnittstelle konfiguriert haben.

  ```
  Created new logical interface hme0:1
  May 24 14:16:53 host1 in.mpathd[101180]:
  Test address now configured on interface hme0;
   enabling probe-based failure detection on it
  ```

Siehe auch Wenn Sie möchten, dass die IPMP-Gruppe über eine Aktiv-Standby-Konfiguration verfügt, setzen Sie mit „So konfigurieren Sie eine Standby-Schnittstelle für eine IPMP-Gruppe“ auf Seite 808 fort.

Konfiguration von Zielsystemen

Die Stichproben-basierte Fehlerkennung beruht auf der Verwendung von Zielsystemen. Dies wird unter „Stichproben-basierte Ausfallerkennung“ auf Seite 790 genauer beschrieben. Für einige IPMP-Gruppen sind die von `in.mpathd` verwendeten Standardziele ausreichend. Für andere IPMP-Gruppen möchten Sie jedoch bestimmte Ziele für die Stichproben-basierte Ausfallerkennung definieren. Sie führen die Stichproben-basierte Ausfallerkennung durch, indem Sie Host-Routen in der Routing-Tabelle als Stichproben-Ziele einrichten. Alle in der Routing-Tabelle konfigurierten Host-Routen werden vor dem Standard-Router aufgeführt. Aus diesem Grund verwendet IPMP die explizit definierten Host-Routen zur Zielauswahl. Zur direkten Angabe von Zielen verwenden Sie eine von zwei Methoden: manuelles Einrichten der Host-Routen oder Erstellen eines Shell-Skripts, das zu einem Startskript wird.

Beachten Sie die folgenden Kriterien bei der Ermittlung, welche Hosts in Ihrem Netzwerk als Ziele geeignet sind.

- Achten Sie darauf, dass die künftigen Ziele verfügbar sind und ausgeführt werden. Erstellen Sie eine Liste ihrer IP-Adressen.
- Stellen Sie sicher, dass sich die Ziel-Schnittstellen im gleichen Netzwerk wie die zu konfigurierenden IPMP-Gruppe befinden.

- Die Netzmasken- und Broadcast-Adresse der Zielsysteme müssen den Adressen in der IPMP-Gruppe gleichen.
- Der Ziel-Host muss in der Lage sein, ICMP-Anforderungen von Schnittstellen zu beantworten, die die Stichproben-basierte Ausfallerkennung verwenden.

▼ So geben Sie Zielsysteme für die Stichproben-basierte Ausfallerkennung manuell an

1 Melden Sie sich mit Ihrem Benutzerkonto bei dem System an, für das Sie eine Stichprobe-basierte Ausfallerkennung konfigurieren möchten.

2 Fügen Sie eine Route zu dem Host hinzu, der als Ziel für die Stichproben-basierte Ausfallerkennung verwendet werden soll.

$ **route add -host** *destination-IP gateway-IP* **-static**

Ersetzen Sie die Werte *Ziel-IP* und *Gateway-IP* durch die IPv4-Adresse des Hosts, der als Ziel verwendet wird. Wenn Sie das Zielsystem `192.168.85.137` angeben möchten, das sich im gleichen Teilnetz wie die Schnittstellen in der IPMP-Gruppe `testgroup1` befindet, geben Sie Folgendes ein:

```
$ route add -host 192.168.85.137 192.168.85.137 -static
```

3 Fügen Sie Routen zu zusätzlichen Hosts im Netzwerk hinzu, die als Zielsysteme verwendet werden.

▼ So geben Sie Zielsysteme in einem Shell-Skript an

1 Nehmen Sie auf dem System, auf dem eine IPMP-Gruppe konfiguriert werden soll, die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie ein Shell-Skript, in dem statische Routen zu den geplanten Zielen eingerichtet werden.

Beispielsweise können Sie ein Shell-Skript namens `ipmp.targets` mit dem folgenden Inhalt erstellen:

```
TARGETS="192.168.85.117 192.168.85.127 192.168.85.137"

case "$1" in
        'start')
            /usr/bin/echo "Adding static routes for use as IPMP targets"
        for target in $TARGETS; do
```

```
      /usr/sbin/route add -host $target $target
        done
                  ;;
        'stop')
              /usr/bin/echo "Removing static routes for use as IPMP targets"
         for target in $TARGETS; do
        /usr/sbin/route delete -host $target $target
         done
                  ;;
esac
```

3. **Kopieren Sie das Shell-Skript in das Verzeichnis für Startskripten.**

   ```
   # cp ipmp.targets /etc/init.d
   ```

4. **Ändern Sie die Berechtigungen für das neue Startskript.**

   ```
   # chmod 744 /etc/init.d/ipmp.targets
   ```

5. **Ändern Sie die Eigentümerschaft für das neue Startskript.**

   ```
   # chown root:sys /etc/init.d/ipmp.targets
   ```

6. **Erstellen Sie einen Link für das Startskript im Verzeichnis** `/etc/init.d`**.**

   ```
   # ln /etc/init.d/ipmp.targets /etc/rc2.d/S70ipmp.targets
   ```

   Das Präfix „S70" im Dateiname `S70ipmp.targets` ordnet das neue Skript korrekt mit Bezug auf die anderen Startskripten ein.

Konfiguration von Standby-Schnittstellen

Verwenden Sie das folgende Verfahren, wenn die IPMP-Gruppe über eine Aktiv-Standby-Konfiguration verfügen soll. Weitere Informationen zu diesem Konfigurationstyp finden Sie unter „IPMP-Schnittstellenkonfigurationen" auf Seite 787.

▼ So konfigurieren Sie eine Standby-Schnittstelle für eine IPMP-Gruppe

Bevor Sie beginnen

- Alle Schnittstellen müssen als Mitglieder der IPMP-Gruppe konfiguriert worden sein.
- Für die Schnittstelle, die zur Standby-Schnittstelle werden soll, darf keine Testadresse konfiguriert worden sein.

Informationen zur Konfiguration einer IPMP-Gruppe und zum Zuweisen von Testadressen finden Sie unter „So konfigurieren Sie eine IPMP-Gruppe mit mehreren Schnittstellen" auf Seite 801.

1. **Nehmen Sie auf dem System mit den zu konfigurierenden Standby-Schnittstellen die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Konfigurieren Sie eine Schnittstelle als eine Standby-Schnittstelle, und weisen Sie eine Testadresse zu.

```
# ifconfig interface plumb \
ip-address other-parameters deprecated -failover standby up
```

Eine Standby-Schnittstelle kann nur eine IP-Adresse aufweisen, die Testadresse. Sie müssen die Option `-failover` einrichten, bevor Sie die Option `standby up` einrichten. Für <andere-Parameter> verwenden Sie die für Ihre Konfiguration erforderlichen Parameter. Lesen Sie dazu die Beschreibung in der Manpage `ifconfig`(1M).

- Um beispielsweise eine IPv4-Testadresse zu erstellen, geben Sie den folgenden Befehl ein:

```
# ifconfig hme1 plumb 192.168.85.22 netmask + broadcast + deprecated -failover standby up
```

`hme1`	Definiert `hme1` als physikalische Schnittstelle, die als Standby-Schnittstelle konfiguriert werden soll.
`192.168.85.22`	Weist der Standby-Schnittstelle diese Testadresse zu.
`deprecated`	Gibt an, dass die Testadresse nicht für abgehende Pakete verwendet wird.
`-failover`	Gibt an, dass die Testadresse kein Failover ausführt, falls die Schnittstelle ausfällt.
`standby`	Kennzeichnet die Schnittstelle als eine Standby-Schnittstelle.

- Zum Erstellen einer IPv6-Testadresse geben Sie den folgenden Befehl ein:

```
# ifconfig hme1 plumb -failover standby up
```

3 Prüfen Sie die Ergebnisse der Konfiguration als Standby-Schnittstelle.

```
# ifconfig hme1
hme1: flags=69040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER,
      STANDBY,INACTIVE mtu 1500
         index 4 inet 192.168.85.22 netmask ffffff00 broadcast 19.16.85.255
         groupname test
```

Das Flag `INACTIVE` kennzeichnet, dass diese Schnittstelle nicht für abgehende Pakete verwendet wird. Falls an dieser Standby-Schnittstelle ein Failover auftritt, wird das Flag `INACTIVE` gelöscht.

Hinweis – Mit dem Befehl `ifconfig` *Schnittstelle* können Sie jederzeit den aktuellen Status einer Schnittstelle anzeigen. Weitere Informationen zum Anzeigen des Schnittstellenstatus finden Sie unter „So zeigen Sie Informationen zu einer bestimmten Schnittstelle an“ auf Seite 221.

---

4 (Optional) Behalten Sie die IPv4-Standby-Schnittstelle nach einem Neustart bei.

Weisen Sie die Standby-Schnittstelle der gleichen IPMP-Gruppe zu, und konfigurieren Sie eine Testadresse für die Standby-Schnittstelle.

Um beispielsweise hme1 als Standby-Schnittstelle zu konfigurieren, fügen Sie die folgende Zeile zur /etc/hostname.hme1-Datei hinzu:

```
192.168.85.22 netmask + broadcast + deprecated group test -failover standby up
```

5 (Optional) Behalten Sie die IPv6-Standby-Schnittstelle nach einem Neustart bei.

Weisen Sie die Standby-Schnittstelle der gleichen IPMP-Gruppe zu, und konfigurieren Sie eine Testadresse für die Standby-Schnittstelle.

Um beispielsweise hme1 als Standby-Schnittstelle zu konfigurieren, fügen Sie die folgende Zeile zur /etc/hostname6.hme1-Datei hinzu:

```
-failover group test standby up
```

Beispiel 31–4 Konfigurieren einer Standby-Schnittstelle für eine IPMP-Gruppe

Angenommen, Sie möchten eine Testadresse mit der folgenden Konfiguration erstellen:

- Physikalische Schnittstelle hme2 als Standby-Schnittstelle
- Testadresse lautet 192.168.85.22
- deprecated- und -failover-Optionen sind gesetzt
- Netzmasken- und Broadcast-Adresse werden auf den Standardwert gesetzt

In diesem Fall geben Sie Folgendes ein:

```
# ifconfig hme2 plumb 192.168.85.22 netmask + broadcast + \
deprecated -failover standby up
```

Die Schnittstelle wird erst dann als eine Standby-Schnittstelle übernommen, nachdem die Adresse als eine NOFAILOVER-Adresse gekennzeichnet wurde.

Sie entfernen den Standby-Status einer Schnittstelle durch Eingabe von:

```
# ifconfig interface -standby
```

Konfiguration von IPMP-Gruppen mit einer physikalischen Schnittstelle

Wenn nur eine Schnittstelle in einer IPMP-Gruppe vorhanden ist, kann kein Failover durchgeführt werden. Sie können jedoch eine Ausfallerkennung für diese Schnittstelle aktivieren, indem Sie die Schnittstelle einer IPMP-Gruppe zuweisen. Für diese Ausfallerkennung müssen Sie keine spezielle IP-Testadresse konfigurieren. Sie können eine einzelne IP-Adresse zum Senden von Daten und Erkennen eines Ausfalls verwenden.

▼ So konfigurieren Sie eine IPMP-Gruppe mit nur einer Schnittstelle

1 Nehmen Sie auf dem System mit der geplanten IPMP-Gruppe mit nur einer Schnittstelle die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 Bei IPv4 erstellen Sie eine IPMP-Gruppe mit nur einer Schnittstelle.

Verwenden Sie die folgende Syntax, um einer IPMP-Gruppe nur eine Schnittstelle zuzuweisen.

 # ifconfig *interface* **group** *group-name*

Das folgende Beispiel weist die Schnittstelle `hme0` der IPMP-Gruppe `v4test` zu:

```
# ifconfig hme0 group v4test
```

Nachdem dieser Schritt durchgeführt wurde, ermöglicht IPMP eine Link-basierte Ausfallerkennung für die Schnittstelle.

Darüber hinaus können Sie den Unterbefehl `-failover` des Befehls `ifconfig` verwenden, um eine stichprobenbasierte Ausfallerkennung durchzuführen. Das folgende Beispiel ermöglicht eine stichprobenbasierte Ausfallerkennnung an `hme0` durch Verwenden der IP-Adresse, die derzeit folgender Schnittstelle zugewiesen ist: `hme0`:

```
# ifconfig hme0 -failover
```

Anders als bei Gruppen mit mehreren Schnittstellen kann die gleiche IP-Adresse sowohl als Daten- als auch als Testadresse verwendet werden. Damit Anwendungen die Testadresse auch als Datenadresse verwenden können, dürfen Testadressen auf IPMP-Gruppen mit nur einer Schnittstelle nie als `deprecated` gekennzeichnet werden.

3 Bei IPv6 erstellen Sie eine IPMP-Gruppe mit nur einer Schnittstelle.

Verwenden Sie die folgende Syntax, um einer IPMP-Gruppe nur eine Schnittstelle zuzuweisen:

 # ifconfig *interface* **inet6 group** *group-name*

Beispiel: Um die einzelne Schnittstelle `hme0` in die IPMP-Gruppe `v6test` einzufügen, geben Sie Folgendes ein:

```
# ifconfig hme0 inet6 group v6test
```

Nachdem dieser Schritt durchgeführt wurde, ermöglicht IPMP eine Link-basierte Ausfallerkennung für die Schnittstelle.

Darüber hinaus können Sie den Unterbefehl `-failover` des Befehls `ifconfig` verwenden, um eine stichprobenbasierte Ausfallerkennung durchzuführen. Das folgende Beispiel ermöglicht

eine stichprobenbasierte Ausfallerkennnung an `hme0` durch Verwenden der IP-Adresse, die derzeit folgender Schnittstelle zugewiesen ist: `hme0`:

```
# ifconfig hme0 inet6 -failover
```

Anders als bei Gruppen mit mehreren Schnittstellen kann die gleiche IP-Adresse sowohl als Daten- als auch als Testadresse verwendet werden. Damit Anwendungen die Testadresse auch als Datenadresse verwenden können, dürfen Testadressen auf IPMP-Gruppen mit nur einer Schnittstelle nie als `deprecated` gekennzeichnet werden.

Bei einer Konfiguration mit einer physikalischen Schnittstelle können Sie nicht überprüfen, ob ein Ausfall des Zielsystems, an das Stichproben gesendet werden oder der Schnittstelle aufgetreten ist. Die Stichproben können nur über eine physikalische Schnittstelle an das Zielsystem gesendet werden. Wenn sich nur ein Standard-Router im Teilnetz befindet, deaktivieren Sie IPMP, falls sich nur eine einzelne physikalische Schnittstelle in der Gruppe befindet. Wenn separate IPv4- und IPv6-Standard-Router vorhanden sind oder mehrere Standard-Router existieren, müssen die Stichproben an mehrere Zielsysteme gesendet werden. In diesem Fall können Sie IPMP sicher aktivieren.

Verwalten von IPMP-Gruppen

In diesem Abschnitt finden Sie Aufgaben zur Verwaltung vorhandener IPMP-Gruppen und der Schnittstellen, die diesen Gruppen zugewiesen sind. Bei dem beschriebenen Aufgaben wird davon ausgegangen, dass bereits eine IPMP-Gruppe konfiguriert ist. Anweisungen hierzu finden Sie unter „Konfiguration von IPMP-Gruppen“ auf Seite 799.

▼ So zeigen Sie die IPMP-Gruppenmitgliedschaft einer Schnittstelle an

1. **Melden Sie sich auf dem System mit der IPMP-Gruppenkonfiguration als Superuser an, oder nehmen Sie eine entsprechende Rolle an.**

   Rollen umfassen Autorisierungen und privilegierte Befehle. Weitere Informationen zu Rollen finden Sie unter „Configuring RBAC (Task Map)“ in *System Administration Guide: Security Services*.

2. **Zeigen Sie Informationen zur Schnittstelle an, einschließlich der Gruppe, zu der die Schnittstelle gehört.**

   ```
   # ifconfig interface
   ```

3. **Wenn anwendbar, zeigen Sie die IPv6-Informationen für die Schnittstelle an.**

   ```
   # ifconfig interface inet6
   ```

Beispiel 31–5 Anzeigen der Gruppen mit physikalischen Schnittstellen

Geben Sie das Folgende ein, um den Gruppennamen für die Schnittstelle `hme0` anzuzeigen:

```
# ifconfig hme0
    hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
      index 2 inet 192.168.85.19 netmask ffffff00 broadcast 192.168.85.255
      groupname testgroup1
```

Um den Gruppennamen nur für die IPv6-Informationen anzuzeigen, geben Sie das Folgende ein:

```
# ifconfig hme0 inet6
    hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
            inet6 fe80::a00:20ff:feb9:19fa/10
            groupname testgroup1
```

▼ So fügen Sie eine Schnittstelle zu einer IPMP-Gruppe hinzu

1. **Nehmen Sie auf dem System mit der IPMP-Gruppenkonfiguration die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Fügen Sie der IPMP-Gruppe die Schnittstelle hinzu.**

   `# ifconfig` *interface* `group` *group-name*

   Die für *Schnittstelle* angegebene Schnittstelle wird Mitglied der IPMP-Gruppe *Gruppenname*.

Beispiel 31–6 Hinzufügen einer Schnittstelle zu einer IPMP-Gruppe

Geben Sie den folgenden Befehl ein, um die Schnittstelle `hme0` zur IPMP-Gruppe `testgroup2` hinzuzufügen:

```
# ifconfig hme0 group testgroup2
  hme0: flags=9000843<UP ,BROADCAST,RUNNING,MULTICAST,IPv4,NOFAILOVER> mtu 1500 index 2
  inet 192.168.85.19 netmask ff000000 broadcast 10.255.255.255
  groupname testgroup2
  ether 8:0:20:c1:8b:c3
```

So entfernen Sie eine Schnittstelle aus einer IPMP-Gruppe

Durch den Befehl `ifconfig` mit dem Parameter `group` und einer Null-Zeichenfolge wird die Schnittstelle aus der aktuellen IPMP-Gruppe entfernt. Seien Sie beim Entfernen von Schnittstellen aus einer Gruppe vorsichtig. Falls eine andere Schnittstelle in der IPMP-Gruppe ausgefallen ist, könnte ein Failover stattgefunden haben. Angenommen, die Schnittstelle `hme0` ist zuvor ausgefallen, so gingen alle Adressen an `hme1` über, vorausgesetzt, `hme1` ist Teil der gleichen Gruppe. Durch Entfernen von `hme1` setzt der `in.mpathd`-Daemon alle Failover-Adressen auf eine andere Schnittstelle in der Gruppe zurück. Wenn keine weitere Schnittstelle in der Gruppe funktioniert, wird bestimmter Netzwerkzugriff durch das Failover nicht wiederhergestellt.

Entsprechend gilt, wenn das Plumbing einer Schnittstelle in der Gruppe aufgehoben wurde, müssen Sie die Schnittstelle zunächst aus der Gruppe entfernen. Dann stellen Sie sicher, dass alle ursprünglichen IP-Adressen für die Schnittstelle konfiguriert sind. Der `in.mpathd`-Daemon versucht, die ursprüngliche Konfiguration einer Schnittstelle, die aus einer Gruppe entfernt wird, wiederherzustellen. Bevor Sie das Plumbing einer Schnittstelle aufheben, müssen Sie sicherstellen, dass die Konfiguration wieder hergestellt wurde. Informationen zum Zustand von Schnittstellen vor und nach einem Failover finden Sie unter „Vorgänge während eines Schnittstellen-Failover“ auf Seite 791.

1. **Nehmen Sie auf dem System mit der IPMP-Gruppenkonfiguration die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Entfernen Sie die Schnittstelle aus der IPMP-Gruppe.**

   ```
   # ifconfig interface group ""
   ```

   Die Anführungszeichen kennzeichnen eine Null-Zeichenfolge.

Beispiel 31–7 Entfernen einer Schnittstelle aus einer Gruppe

Geben Sie den folgenden Befehl ein, um die Schnittstelle `hme0` aus der IPMP-Gruppe `test` zu entfernen:

```
# ifconfig hme0 group ""
    # ifconfig hme0
    hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
    index 2 inet 192.168.85.19 netmask ffffff00 broadcast 192.168.85.255
    # ifconfig hme0 inet6
```

```
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
inet6 fe80::a00:20ff:feb9:19fa/10
```

▼ So verschieben Sie eine Schnittstelle von einer IPMP-Gruppe in eine andere

Sie können eine Schnittstelle in eine neue IPMP-Gruppe verschieben, wenn die Schnittstelle einer existierenden IPMP-Gruppe angehört. Dazu müssen Sie die Schnittstelle nicht aus der aktuellen IPMP-Gruppe entfernen. Wenn Sie die Schnittstelle in eine neue Gruppe einfügen, wird sie automatisch aus der existierenden IPMP-Gruppe entfernt.

1. **Nehmen Sie auf dem System mit der IPMP-Gruppenkonfiguration die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Verschieben Sie eine Schnittstelle in eine neue IPMP-Gruppe.**

   ```
   # ifconfig interface group group-name
   ```

   Durch das Einfügen der Schnittstelle in einer neuen Gruppe wird sie automatisch aus einer vorhandenen Gruppe entfernt.

Beispiel 31–8 Verschieben einer Schnittstelle in eine andere IPMP-Gruppe

Geben Sie das Folgende ein, um die IPMP-Gruppe der Schnittstelle `hme0` zu ändern:

```
# ifconfig hme0 group cs-link
```

Mit diesem Befehl entfernen Sie die Schnittstelle `hme0` aus der IPMP-Gruppe `test` und fügen die Schnittstelle dann der Gruppe `cs-link` hinzu.

Ersetzen einer ausgefallenen physikalischen Schnittstelle auf Systemen, die DR unterstützen

In diesem Abschnitt finden Sie Verfahren zur Verwaltung von Systemen, die eine dynamische Rekonfiguration (DR) unterstützen.

Hinweis – Diese Aufgaben beziehen sich nur auf IP-Schichten, die mithilfe des Befehls `ifconfig` konfiguriert wurden. Schichten über oder unter der IP-Schicht, z. B. ATM oder andere Services, erfordern spezielle manuelle Schritte, falls die Schichten nicht automatisiert sind. Die Schritte im folgenden Verfahren dienen zum Dekonfigurieren von Schnittstellen als Vorbereitung zum Trennen und Konfigurieren der Schnittstellen nach dem Wiederanschließen.

▼ So entfernen Sie eine ausgefallene physikalische Schnittstelle (DR-Detach)

In diesem Verfahren wird gezeigt, wie Sie eine physikalische Schnittstelle von einem System entfernen, das DR unterstützt. Es wird davon ausgegangen, dass die folgenden Bedingungen bestehen:

- Die physikalischen Schnittstellen `hme0` und `hme1` sind die Beispielschnittstellen.
- Beide Schnittstellen befinden sich in der gleichen IPMP-Gruppe.
- `hme0` ist ausgefallen.
- Die logische Schnittstelle `hme0:1` besitzt die Testadresse.
- Sie ersetzen die ausgefallene Schnittstelle durch den gleichen physikalischen Schnittstellennamen, z. B. `hme0` durch `hme0`.

Hinweis – Sie können Schritt 2 überspringen, wenn die Testadresse mithilfe der Datei `/etc/hostname.hme0` geplumbt wurde.

---

1. **Nehmen Sie auf dem System mit der IPMP-Gruppenkonfiguration die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Zeigen Sie die Testadressenkonfiguration an.**

```
# ifconfig hme0:1

hme0:1:
flags=9040842<BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
mtu 1500 index 3
inet 192.168.233.250 netmask ffffff00 broadcast 192.168.233.255
```

   Sie benötigen diese Informationen, um die Testadresse nach dem Ersetzen der physikalischen Schnittstelle erneut zu plumben.

3 Entfernen Sie die physikalische Schnittstelle.

Eine vollständige Beschreibung zum Entfernen einer physikalischen Schnittstelle finden Sie in den folgenden Quellen:

- Manpage `cfgadm`(1M)
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*
- *Sun Enterprise 10000 DR Configuration Guide*

▼ So ersetzen Sie eine ausgefallene physikalische Schnittstelle (DR-Attach)

In diesem Verfahren wird gezeigt, wie Sie eine physikalische Schnittstelle auf einem System ersetzen, das DR unterstützt.

1 Nehmen Sie auf dem System mit der IPMP-Gruppenkonfiguration die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Ersetzen Sie die physikalische Schnittstelle.

Anweisungen hierzu finden Sie in den folgenden Quellen:

- Manpage `cfgadm`(1M)
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*
- *Sun Enterprise 10000 DR Configuration Guide*, or *Sun Fire 880 Dynamic Reconfiguration User's Guide*

Wiederherstellung einer physikalischen Schnittstelle, die beim Systemstart nicht vorhanden war

---

Hinweis – Das folgende Verfahren gilt nur für IP-Schichten, die mithilfe des Befehls `ifconfig` konfiguriert wurden. Schichten über oder unter der IP-Schicht, z. B. ATM oder andere Services, erfordern spezielle manuelle Schritte, falls die Schichten nicht automatisiert sind. Die besonderen Schritte im folgenden Verfahren dienen zum Dekonfigurieren von Schnittstellen als Vorbereitung zum Trennen und Konfigurieren der Schnittstellen nach dem Wiederanschließen.

Die Wiederherstellung nach einer dynamischen Rekonfiguration wird automatisch für eine Schnittstelle durchgeführt, die Teil eines I/O-Boards auf einer Sun Fire™-Plattform ist. Handelt es sich bei der NIC um ein Sun Crypto Accelerator I - cPCI-Board, erfolgt die Wiederherstellung ebenfalls automatisch. Folglich sind die folgenden Schritte nicht für eine Schnittstelle erforderlich, die im Rahmen eines DR-Vorgangs wiederhergestellt werden. Weitere Informationen zu den Systemen Sun Fire x800 und Sun Fire 15000 finden Sie in der Manpage `cfgadm_sbd(1M)` Die physikalische Schnittstelle für ein Failback auf die Konfiguration aus, die in der `/etc/hostname.` *Schnittstelle*-Datei angegeben ist. Informationen zur Konfiguration von Schnittstellen, die ihre Konfiguration auch nach einem Neustart beibehalten, finden Sie unter „Konfiguration von IPMP-Gruppen“ auf Seite 799.

Hinweis – Bei Sun Fire Legacy (Exx00)-Systemen werden DR-Detachments noch immer manuell vorgenommen. DR-Attachments sind jedoch automatisiert.

▼ So stellen Sie eine physikalische Schnittstelle wieder her, die beim Systemstart nicht vorhanden war

Sie müssen das folgende Verfahren vollständig abschließen, bevor Sie eine physikalische Schnittstelle wiederherstellen können, die beim Systemstart nicht vorhanden war. Das Beispiel in diesem Verfahren hat die folgende Konfiguration:

- Die physikalischen Schnittstellen `hme0` und `hme1` sind die Beispielschnittstellen.
- Beide Schnittstellen befinden sich in der gleichen IPMP-Gruppe.
- `hme0` war beim Systemstart nicht vorhanden.

Hinweis – Das Failback von IP-Adressen während der Wiederherstellung einer ausgefallenen physikalischen Schnittstelle dauert bis zu 3 Minuten. Diese Zeit kann je nach Netzverkehr variieren. Außerdem hängt sie von der Stabilität der eingehenden Schnittstelle beim Failback der Failover-Schnittstellen vom `in.mpathd`-Daemon ab.

---

1. **Nehmen Sie auf dem System mit der IPMP-Gruppenkonfiguration die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Rufen Sie die Informationen zum ausgefallenen Netzwerk aus der Ausfall-Fehlermeldung im Konsolenprotokoll ab.**

   Weitere Informationen finden Sie in der Manpage `syslog`(3C) Die Fehlermeldung könnte wie folgt angezeigt werden:

   ```
   moving addresses from failed IPv4 interfaces:
   hme1 (moved to hme0)
   ```

   Diese Meldung gibt an, dass die IPv4-Adressen der ausgefallenen Schnittstelle `hme1` ein Failover auf die Schnittstelle `hme0` durchgeführt haben.

   Alternativ empfangen Sie die folgende Meldung:

   ```
   moving addresses from failed IPv4 interfaces:
   hme1 (couldn't move, no alternative interface)
   ```

   Diese Meldung kennzeichnet, dass keine aktive Schnittstelle in der gleichen Gruppe wie die ausgefallene Schnittstelle `hme1` gefunden wurde. Aus diesem Grund konnte kein Failover für die IPv4-Adressen von `hme1` durchgeführt werden.

3. **Schließen Sie die physikalische Schnittstelle im System an.**

   Anweisungen zum Ersetzen einer physikalischen Schnittstelle finden Sie in den folgenden Quellen:

   - Manpage `cfgadm`(1M)
   - *Sun Enterprise 10000 DR Configuration Guide*
   - *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*

4. **Siehe Meldung aus Schritt 2. Gehen Sie zu Schritt 6, wenn die Adressen nicht verschoben werden konnten. Gehen Sie zu Schritt 5, wenn die Adressen verschoben wurden.**

5 Heben Sie das Plumbing der logischen Schnittstellen auf, die im Rahmen des Failover-Prozesses konfiguriert wurden.

a. Lesen Sie den Inhalt der `/etc/hostname.`*verschoben-von-Schnittstelle***-Datei, um festzustellen, welche logischen Schnittstellen im Rahmen des Failover-Prozesses konfiguriert wurden.**

b. Heben Sie das Plumbing aller Failover-IP-Adressen auf.

`# ifconfig` *moved-to-interface* `removeif` *moved-ip-address*

Hinweis – Failover-Adressen sind mit dem Parameter `failover` markiert oder mit dem Parameter `-failover` nicht markiert. Bei IP-Adressen, die mit dem Parameter `-failover` markiert sind, muss das Plumbing nicht aufgehoben werden.

Angenommen, die Datei `/etc/hostname.hme0` enthält die folgenden Zeilen:

```
inet 10.0.0.4 -failover up group one
addif 10.0.0.5 failover up
addif 10.0.0.6 failover up
```

Um alle Failover-IP-Adressen zu löschen, geben Sie die folgenden Befehle ein:

```
# ifconfig hme0 removeif 10.0.0.5
# ifconfig hme0 removeif 10.0.0.6
```

6 Konfigurieren Sie die IPv4-Informationen für die ersetzte physikalische Schnittstellen neu, indem Sie den folgenden Befehl für jede entfernte Schnittstelle eingeben:

`# ifconfig` *removed-from-NIC* `<parameters>`

Beispielsweise können Sie die folgenden Befehle eingeben:

```
# ifconfig hme1 inet plumb
# ifconfig hme1 inet 10.0.0.4 -failover up group one
# ifconfig hme1 addif 10.0.0.5 failover up
# ifconfig hme1 addif 10.0.0.6 failover up
```

Ändern von IPMP-Konfigurationen

In der IPMP-Konfigurationsdatei `/etc/default/mpathd` werden die folgenden systemweit geltenden Parameter für IPMP-Gruppen konfiguriert.

- `FAILURE_DETECTION_TIME`
- `TRACK_INTERFACES_ONLY_WITH_GROUPS`
- `FAILBACK`

▼ So konfigurieren Sie die `/etc/default/mpathd`-Datei

1 Nehmen Sie auf dem System mit der IPMP-Gruppenkonfiguration die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser an.

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Bearbeiten Sie die Datei `/etc/default/mpathd`**.**

Ändern Sie den Standardwert eines oder mehrerer der drei Parameter.

a. Geben Sie den neuen Wert für den Parameter `FAILURE_DETECTION_TIME` **ein.**

`FAILURE_DETECTION_TIME=`*n*

n ist die Zeit in Sekunden für ICMP-Stichproben, um zu erkennen, ob eine Schnittstelle ausgefallen ist. Der Standardwert beträgt 10 Sekunden.

b. Geben Sie einen neuen Wert für den Parameter `FAILBACK` **ein.**

`FAILBACK=[yes | no]`

- *yes* - Der Wert *yes* ist das Standard-Failback-Verhalten für IPMP. Wenn die Reparatur einer ausgefallenen Schnittstelle erkannt wird, findet ein Failback-Prozess des Netzwerkzugriffs auf die reparierte Schnittstelle statt. Dies wird unter „IPMP-Funktionen zur Ausfall- und Reparaturerkennung“ auf Seite 789 ausführlich beschrieben.
- *no* - Der Wert *no* gibt an, dass Datenverkehr kein Failback auf eine reparierte Schnittstelle durchführt. Wenn eine ausgefallene Schnittstelle als repariert erkannt wird, wird das Flag *INACTIVE* für diese Schnittstelle gesetzt. Dieses Flag weist darauf hin, dass die Schnittstelle derzeit nicht für Datenverkehr verwendet wird. Die Schnittstelle kann dennoch für Stichprobenverkehr verwendet werden.

  Angenommen, eine IPMP-Gruppe besteht aus zwei Schnittstellen, ce0 und ce1. Der Wert *FAILBACK=no* ist in der Datei `/etc/default/mpathd` eingerichtet. Wenn ce0 ausfällt, führt dessen Datenverkehr ein Failover auf ce1 durch. Dies ist das erwartete Standardverhalten von IPMP. Wenn IPMP jedoch erkennt, dass ce0 repariert wurde, findet kein Failback von ce1 statt, da der Parameter *FAILBACK=no* in der Datei `/etc/default/mpathd` eingerichtet ist. Die Schnittstelle ce0 behält den Status `INACTIVE` bei und wird nicht für Datenverkehr verwendet, es sei denn, die Schnittstelle ce1 fällt aus. Falls die Schnittstelle ce1 ausfällt, werden die Adressen von ce1 zurück zu ce0 migriert, dessen Flag INACTIVE gelöscht wird. Diese Migration findet nur dann statt, wenn ce0 die einzige Schnittstelle mit dem Flag INACTIVE in der Gruppe ist. Falls weitere INACTIVE-Schnittstellen in der Gruppe vorhanden sind, migrieren die Adressen eventuell zu einer anderen INACTIVE-Schnittstelle als ce0.

c. **Geben Sie den neuen Wert für den Parameter** `TRACK_INTERFACES_ONLY_WITH_GROUPS` **ein.**

```
TRACK_INTERFACES_ONLY_WITH_GROUPS=[yes | no]
```

- *yes* - Der Wert *yes* ist das Standardverhalten für IPMP. Dieser Parameter führt dazu, dass IPMP Netzwerkschnittstellen ignoriert, die nicht in einer IPMP-Gruppe konfiguriert sind.
- *no* - Der Wert *no* richtet eine Ausfall- oder Reparaturerkennung für *alle* Netzwerkschnittstellen ein, unabhängig davon, ob sie in einer IPMP-Gruppe konfiguriert sind. Wird ein Ausfall oder eine Reparatur einer Schnittstelle erkannt, die nicht in einer IPMP-Gruppe konfiguriert ist, findet kein Failover oder Failback statt. Aus diesem Grund eignet sich der Wert *no* nur zum Anzeigen von Ausfällen und führt zu keiner Verbesserung der Netzwerkverfügbarkeit.

3 **Starten Sie den** `in.mpathd`**-Daemon neu.**

```
# pkill -HUP in.mpathd
```

TEIL VII

IP Quality of Service (IPQoS)

Dieser Teil enthält Aufgaben und Informationen zum IP Quality of Service (IPQoS), der Umsetzung von Differentiated Services in Oracle Solaris.

KAPITEL 32

Einführung in IPQoS (Übersicht)

Mit IP Quality of Service (IPQoS) können Sie Accounting-Statistiken sammeln, steuern und priorisieren. IPQoS bietet den Benutzern Ihres Netzwerks konsistente Serviceebenen. Darüber hinaus können Sie den Datenverkehr verwalten, um Netzwerküberlastungen zu vermeiden.

Dieses Kapitel umfasst die folgenden Themen:

- „Grundlagen von IPQoS“ auf Seite 825
- „Bereitstellen von Quality of Service mit IPQoS“ auf Seite 828
- „Verbessern der Netzwerkeffizienz mit IPQoS“ auf Seite 829
- „Differentiated Services-Modell“ auf Seite 831
- „Verkehrsweiterleitung in einem IPQoS-konformen Netzwerk“ auf Seite 836

Grundlagen von IPQoS

IPQoS ermöglicht die Differentiated Services (Diffserv)-Architektur, die von der Differentiated Services Working Group der Internet Engineering Task Force (IETF) definiert wurde. Unter Oracle Solaris wird IPQoS auf der IP-Schicht im TCP/IP-Protokollstapel implementiert.

Was sind Differentiated Services?

Durch Aktivieren von IPQoS können Sie ausgewählten Kunden und Anwendungen unterschiedliche Ebenen an Netzwerkservices anbieten. Diese unterschiedlichen Serviceebenen werden kollektiv als *Differentiated Services* (differenzierte Dienste) bezeichnet. Die Differentiated Services, die Sie Ihren Kunden bereitstellen, können auf verschiedenen Serviceebenen basieren, die Ihr Unternehmen seinen Kunden anbietet. Sie können Differentiated Services auch basierend auf Prioritäten anbieten, die für Anwendungen oder Benutzer in Ihrem Netzwerk eingerichtet wurden.

Das Bereitstellen von QoS umfasst die folgenden Aktivitäten:

- Delegieren von Serviceebenen zu einzelnen Gruppen, z. B. Kunden oder Abteilungen in einem Unternehmen
- Priorisieren von Netzwerkservices, die bestimmten Gruppen oder Anwendungen bereitgestellt werden
- Erkennen und Eliminieren von Netzwerkengpässen und anderen Formen von Überlastungen
- Überwachen der Netzwerkleistung und Bereitstellen von Leistungsstatistiken
- Regulieren der Bandbreite zu Netzwerkressourcen

Funktionen von IPQoS

IPQoS bietet die folgenden Funktionen:

- `ipqosconf`-Befehlszeilentool zur Konfiguration der QoS-Richtlinie
- Classifier, die Aktionen auswählen, die wiederum auf Filtern basieren, mit denen die QoS-Richtlinie Ihrer Organisation definiert wird
- Metermodul, mit dem der Netzverkehr in Übereinstimmung mit dem Diffserv-Modell gemessen wird
- Service-Differenzierung, die auf der Fähigkeit basiert, den IP-Header eines Pakets mit Weiterleitungsinformationen zu kennzeichnen
- Flow Accounting-Modul, das Statistiken über den Verkehrswert sammelt
- Erfassung von Statistiken zu Verkehrsklassen über den UNIX®-Befehl `kstat`
- Unterstützung für SPARC®- und x86-Architekturen
- Unterstützung der IPv4- und IPv6-Adressierung
- Interoperabilität mit IP Security Architecture (IPsec)
- Unterstützung für 802.1D Markierungen gemäß Benutzer-Priorität für virtuelle lokale Netzwerke (VLANs)

Weitere Informationen zur Theorie und Praxis von Quality-of-Service

Weitere Informationen zu Differentiated Services und Quality Of Service finden Sie in gedruckten Medien und online.

Bücher zu Quality of Service

Weitere Informationen zur Theorie und Praxis von Quality of Service finden Sie in den folgenden Büchern:

- Ferguson, Paul and Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

Requests for Comments (RFCs) zu Quality of Service

IPQoS entspricht den Spezifikationen, die in den folgenden RFCs und den aufgeführten Internet Drafts beschrieben sind:

- RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv 6 Headers (`http://www.ietf.org/rfc/rfc2474.txt?number=2474`) – Beschreibt eine Verbesserung am Type of Service (ToS)-Feld oder den DS-Feldern der IPv4- und IPv6-Paket-Header zur Unterstützung von Differentiated Services
- RFC 2475, An Architecture for Differentiated Services (`http://www.ietf.org/rfc/rfc2475.txt?number=2475`) – Eine ausführliche Beschreibung des Aufbaus und der Module der Diffserv-Architektur
- RFC 2597, Assured Forwarding PHB Group (`http://www.ietf.org/rfc/rfc2597.txt?number=2597`) – Beschreibt, wie das Assured Forwarding (AF) Per-Hop-Verhalten funktioniert.
- RFC 2598, An Expedited Forwarding PHB (`http://www.ietf.org/rfc/rfc2598.txt?number=2598`) – Beschreibt, wie das Expedited·Forwarding (EF) Per-Hop-Verhalten funktioniert.
- Internet-Draft, *An Informal Management Model for Diffserv Routers* – Präsentiert ein Modell zur Umsetzung der Diffserv-Architektur auf Routern.

Websites mit Informationen zu Quality of Service

Die Differentiated Services Working Group der IETF unterhält eine Website mit Links zu Diffserv Internet Drafts unter `http://www.ietf.org/html.charters/diffserv-charter.html`.

Router-Hersteller wie Cisco Systems und Juniper Networks stellen auf ihren Firmen-Websites Informationen bereit, wie Differentiated Services in ihren Produkten umgesetzt sind.

Manpages zu IPQoS

Die IPQoS-Dokumentation umfasst die folgenden Manpages:

- `ipqosconf`(1M) - Beschreibt den Befehl zum Einrichten der IPQoS-Konfigurationsdatei
- `ipqos`(7ipp) – Beschreibt die IPQoS-Umsetzung des Diffserv-Architekturmodells
- `ipgpc`(7ipp) – Beschreibt die IPQoS-Umsetzung eines Diffserv-Classifiers
- `tokenmt`(7ipp) – Beschreibt den IPQoS `tokenmt`-Meter
- `tswtclmt`(7ipp) – Beschreibt den IPQoS `tswtclmt`-Meter

- dscpmk(7ipp) – Beschreibt das DSCP-Markermodul
- dlcosmk(7ipp) – Beschreibt das IPQoS 802.1D Benutzerpriorität-Markermodul
- flowacct(7ipp)– Beschreibt das IPQoS Flow Accounting-Modul
- acctadm(1M) – Beschreibt den Befehl, mit dem die erweiterten Accounting-Funktionen von Oracle Solaris konfiguriert werden. Der Befehl `acctadm` umfasst IPQoS-Erweiterungen.

Bereitstellen von Quality of Service mit IPQoS

Mit IPQoS-Funktionen können Internet Service Providers (ISPs) und Application Service Providers (ASPs) ihren Kunden individuelle Netzwerkservices anbieten. Diese Funktionen ermöglichen es einzelnen Unternehmen und Bildungsinstituten, Services für interne Organisationen oder wichtige Anwendungen zu priorisieren.

Umsetzen von Service-Level Agreements

Handelt es sich bei Ihrer Organisation um einen ISP oder ASP, können Sie Ihre IPQoS-Konfiguration auf dem *Service-Level Agreement* (SLA) basieren, dass Ihr Unternehmen seinen Kunden anbietet. In einer SLA garantiert ein Service Provider einem Kunden einen bestimmten Umfang an Netzwerkservices, die nach einer Preisstruktur abgerechnet wird. Beispielsweise stellt eine SLA im oberen Preisbereich sicher, dass ein Kunde 24 Stunden am Tag die höchste Priorität für alle Arten von Netzwerkverkehr genießt. Entsprechend garantiert eine SLA im mittleren Preisbereich einem Kunden hohe Priorität für E-Mails während der Arbeitszeiten. Sonstiger Netzverkehr erfolgt 24 Stunden am Tag mit mittlerer Priorität.

Sicherstellen des Quality of Service für eine einzelne Organisation

Handelt es sich bei Ihrer Organisation um ein Unternehmen oder eine Institution, können Sie auch für Ihr Netzwerk QoS-Funktionen bereitstellen. Sie können garantieren, dass Datenverkehr einer bestimmten Gruppe oder einer bestimmten Anwendung eine höhere oder niedrigere Servicequalität erhält.

Einführung in die Quality of Service-Richtlinie

Sie implementieren die Quality Of Service, indem Sie eine *Quality of Service (QoS)-Richtlinie* definieren. Die QoS-Richtlinie definiert verschiedene Netzwerkattribute, z. B. die Priorität des Kunden oder der Anwendung sowie Aktionen zur Handhabung verschiedener Kategorien von Datenverkehr. Die QoS-Richtlinie Ihrer Organisation wird in einer IPQoS-Konfigurationsdatei

implementiert. Diese Datei konfiguriert die IPQoS-Module, die sich im Kernel von Oracle Solaris befinden. Ein Host mit einer übernommenen IPQoS-Richtlinie wird als ein *IPQoS-konformes System* bezeichnet.

Ihre QoS-Richtlinie definiert in der Regel Folgendes:

- Diskrete Netzverkehr-Gruppen, die als *Serviceklassen* bezeichnet werden.
- Metriken zur Regulierung der Menge an Netzverkehr für jede Klasse. Diese Metriken überwachen den Prozess zur Messung des Datenverkehrs, der als *Metering* (Zählung) bezeichnet wird.
- Eine Aktion, die ein IPQoS-System und ein Diffserv-Router an einem Paketfluss ausführen muss. Diese Aktion wird als *Per-Hop-Behaviour* (PHB) bezeichnet.
- Alle Statistiken, die von Ihrer Organisation für eine Serviceklasse gesammelt werden. Ein Beispiel ist der Datenverkehr, der von einem Kunden oder einer bestimmten Anwendung erzeugt wird.

Bei Paketen, die an Ihr Netzwerk übergeben werden, wertet das IPQoS-konforme System die Paket-Header aus. Ihre QoS-Richtlinie legt dann die Aktion fest, die das IPQoS-System ausführt.

Aufgaben zum Aufstellen der QoS-Richtlinie sind unter „Planen der Quality of Service-Richtlinie“ auf Seite 845 beschrieben.

Verbessern der Netzwerkeffizienz mit IPQoS

IPQoS enthält Funktionen, die nach der Umsetzung des Quality of Service die Netzwerkperformance verbessern können. Wenn Computernetzwerke wachsen, steigt auch der Bedarf zur Verwaltungsaufwand des Netzverkehrs, der durch eine steigende Anzahl von Benutzern und leistungsstärkeren Prozessoren erzeugt wird. Symptome eines überanspruchten Netzwerks sind z. B. Datenverluste und Überlastung. Beide Symptome führen zu schlechteren Reaktionszeiten.

In der Vergangenheit haben Systemadministratoren Netzverkehrprobleme durch Erhöhen der Bandbreite gelöst. Häufig variiert der Verkehr auf den Links stark. Mit IPQoS können Sie Datenverkehr im vorhandenen Netzwerk verwalten und besser beurteilen, wo und warum eine Erweiterung erforderlich ist.

Bei einem Unternehmen oder einer Institution müssen Sie beispielsweise für ein effizientes Netzwerk sorgen, um Netzwerkengpässe zu vermeiden. Außerdem müssen Sie sicherstellen, dass eine Gruppe oder Anwendung nicht mehr als die zugewiesene Bandbreite verbraucht. Als ISP oder ASP müssen Sie die Netzwerkperformance verwalten, um sicherzustellen, dass Kunden den Netzwerkservice erhalten, für den sie bezahlen.

So wirkt sich die Bandbreite auf den Netzwerkverkehr aus

Mit IPQoS können Sie die Netzwerk*bandbreite* regulieren, die Höchstmenge an Daten, die ein vollständig genutzter Netzwerklink bzw. ein vollständig ausgelastetes Netzwerkgerät übertragen kann. Ihre QoS-Richtlinie muss die Verwendung der Bandbreite priorisieren, um Kunden oder Benutzern einen bestimmten Quality of Service bereitstellen zu können. Die IPQoS-Metermodule ermöglichen Ihnen das Zählen und Steuern der zugewiesenen Bandbreite zwischen den verschiedenen Verkehrsklassen auf einem IPQoS-konformen Host.

Bevor Sie den Verkehr in Ihrem Netzwerk effizient verwalten können, müssen Sie die folgenden Fragen zur Nutzung der Bandbreite beantworten:

- Welches sind die Bereiche mit Verkehrsprobleme in Ihren lokalen Netzwerk?
- Was müssen Sie tun, um die verfügbare Bandbreite optimal nutzen zu können?
- Welches sind die kritischen Anwendungen an Ihren Standort, und welche Anwendung muss die höchste Priorität erhalten?
- Welche Anwendungen reagieren empfindlich auf Überlastung?
- Welches sind die weniger kritischen Anwendungen an Ihren Standort, und welchen Anwendungen kann eine niedrigere Priorität zugewiesen werden?

Verwenden von Serviceklassen zum Priorisieren von Verkehr

Bei der Umsetzung eines Quality of Service analysieren Sie den Netzwerkverkehr, um breite Gruppierungen festzulegen, in die der Netzverkehr aufgeteilt werden kann. Darum strukturieren Sie die verschiedenen Gruppierungen in Serviceklassen mit individuellen Eigenschaften und Prioritäten. Diese Klassen bilden die grundlegenden Kategorien, auf denen Sie die QoS-Richtlinie für Ihrer Organisation basieren. Die Serviceklassen stellen die Verkehrsgruppen dar, die Sie steuern möchten.

Als Provider können Sie beispielsweise die Serviceebenen Platin, Gold, Silber und Bronze mit einer entsprechenden gleitenden Preisstruktur anbieten. Eine Platin-SLA garantiert oberste Priorität für eingehenden Verkehr, dessen Ziel eine Website ist, die der ISP für den Kunden hostet. Somit stellt eingehender Verkehr zur Webseite dieses Kunden eine Verkehrsklasse dar.

Bei einem Unternehmen können Sie Serviceklassen erstellen, die auf den Anforderungen einer Abteilung beruhen. Oder Sie erstellen eine Klasse, die auf der am meisten genutzten Anwendung im Netzwerkverkehr basiert. Im Folgenden sind einige Verkehrsklassen eines Unternehmens aufgeführt:

- Beliebte Anwendungen wie E-Mail und abgehendes FTP an einen bestimmten Server können jeweils eine Klasse bilden. Da Angestellte diese Anwendungen ständig verwenden, kann Ihre QoS-Richtlinie E-Mail- und abgehendem FTP-Verkehr einen geringen Betrag der Bandbreite und eine geringe Bandbreite garantieren.
- Die Datenbank zur Aufnahme von Bestellungen muss 24 Stunden am Tag ausgeführt werden. Abhängig von der Wichtigkeit der Datenbankanwendung für das Unternehmen können Sie der Datenbank einen großen Anteil der Bandbreite und eine hohe Priorität zuweisen.
- Eine Abteilung, die entscheidende oder sensible Arbeiten ausführt, wie die Lohn- und Gehaltsabteilung. Die Wichtigkeit der Abteilung für das Unternehmen wird durch die Priorität und den Anteil an der Bandbreite bestimmt, den Sie dieser Abteilung zuweisen.
- Eingehende Aufrufe der externen Website eines Unternehmens. Sie können dieser Klasse einen mittleren Anteil an der Bandbreite zuweisen, die mit niedriger Priorität ausgeführt wird.

Differentiated Services-Modell

IPQoS umfasst die folgenden Module, die Teil der in RFC 2475 definierten *Differentiated Services (Diffserv)*-Architektur sind:

- Classifier (Klassierer)
- Meter (Zähler)
- Marker (Zeiger)

IPQoS fügt die folgenden Verbesserungen zum Diffserv-Modell hinzu:

- Flow Accounting-Modul
- 802.1D-Datagramm-Marker

In diesem Abschnitt finden Sie eine Einführung in die vom IPQoS verwendeten Diffserv-Module. Zum Einrichten dieser Module in der QoS-Richtlinie müssen Sie mit den Grundlagen zu diesen Modulen vertraut sein und ihre Namen sowie die Verwendungsweise kennen. Ausführliche Informationen zu jedem Modul finden Sie unter „IPQoS-Architektur und das Diffserv-Modell“ auf Seite 907.

Classifier (`ipgpc`) – Übersicht

Bei dem Diffserv-Modell wählt der *Classifier* die Pakete aus dem Netzwerk-Verkehrswert aus. Ein *Verkehrswert* besteht aus einer Paketgruppe mit identischen Informationen in den folgenden IP-Header-Feldern:

- Quelladresse
- Zieladresse

- Ursprungs-Port
- Ziel-Port
- Protokollnummer

Bei IPQoS werden diese Felder als *5-Tuple* bezeichnet.

Das IPQoS-Classifier-Modul heißt `ipgpc`. Der `ipgpc`-Classifier ordnet den Verkehrswert in Klassen an, die auf den Eigenschaften basieren, die Sie in der IPQoS-Konfigurationsdatei definiert haben.

Ausführliche Informationen zu `ipgpc` finden Sie unter „Classifier-Modul“ auf Seite 907.

IPQoS-Klassen

Eine *Klasse* ist eine Gruppe von Netzwerk-Datenströmen mit ähnlichen Eigenschaften. Beispielsweise kann ein ISP Klassen definieren, um die verschiedenen Serviceebenen zu unterscheiden, die den Kunden angeboten werden. Ein ASP könnte SLAs definieren, um verschiedenen Anwendungen unterschiedliche Serviceebenen zuzuweisen. In der QoS-Richtlinie eines ASP könnte eine Klasse abgehenden FTP-Verkehr enthalten, der an eine bestimmte IP-Zieladresse gerichtet ist. Auch von der externen Website eines Unternehmens abgehender Verkehr könnte als eine Klasse definiert sein.

Das Gruppieren von Netzverkehr in Klassen ist ein wichtiger Teil bei der Planung Ihrer QoS-Richtlinie. Wenn Sie Klassen mithilfe des Serviceprogramms `ipqosconf` erstellen, konfigurieren Sie in Wirklichkeit den `ipgpc`-Classifier.

Informationen zum Definieren von Klassen finden Sie unter „So definieren Sie die Klassen für Ihre QoS-Richtlinie“ auf Seite 848.

IPQoS-Filter

Filter sind Regellisten mit Parametern, die als *Selektoren* bezeichnet werden. Jeder Filter muss auf eine Klasse verweisen. IPQoS prüft auf die Übereinstimmung von Paketen mit den Selektoren eines Filters, um festzustellen, ob das Paket zur Klasse des Filters gehört. Sie können ein Paket mithilfe verschiedener Selektoren filtern, beispielsweise dem IPQoS 5-Tuple und anderen allgemeinen Parametern:

- Quell- und Zieladressen
- Ursprungs- und Ziel-Port
- Protokollnummern
- Benutzer-IDs
- Projekt-IDs
- Differentiated Services Codepoint (DSCP)
- Schnittstellenindex

So kann ein einfaches Filter beispielsweise das Zielport mit dem Wert 80 enthalten. The `ipgpc`-Classifier wählt dann alle für Port 80 (HTTP) bestimmten Datenpakete aus und verarbeitet diese gemäß der QoS-Richtlinien.

Informationen zum Erstellen von Filtern finden Sie unter „So definieren Sie Filter in der QoS-Richtlinie" auf Seite 851.

Meter (tokenmt und tswtclmt) – Übersicht

Im Diffserv-Modell verfolgt ein *Meter* die Übertragungsrate des Verkehrswerts auf Klassenbasis. Der Meter wertet aus, inwieweit die tatsächliche Flussrate der konfigurierten Rate entspricht, um das geeignete Ergebnis zu ermitteln. Basierend auf dem Verkehrswert-Ergebnis wählt der Meter eine geeignete Aktion. Dies kann z. B. das Senden des Pakets an eine andere Aktion oder die Rückgabe des Pakets an das Netzwerk ohne weitere Verarbeitung sein.

Die IPQoS-Metermodule bestimmen, ob ein Netzwerkfluss der Übertragungsrate entspricht, die in der QoS-Richtlinie für diese Klasse definiert wurde. IPQoS umfasst zwei Metermodule:

- `tokenmt` – Verwendet einen zwei-Token Bucket-Zähler
- `tswtclmt` – Verwendet einen Timesliding-Window-Zähler

Beide Metermodule erkennen drei Ergebnisse: Rot, Gelb und Grün. Die Aktionen, die bei den verschiedenen Ergebnissen durchzuführen sind, werden mit den Parametern `red_action_name`, `yellow_action_name` und `green_action_name` definiert.

Darüber hinaus können Sie `tokenmt` zum Erkennen von Farben konfigurieren. Ein farbbewusster Meter verwendet Paketgröße, DSCP, Traffic Rate und konfigurierte Parameter, um das Ergebnis festzustellen. Der Meter verwendet das DSCP, um das Ergebnis des Pakets entweder grün, gelb oder rot zuzuordnen.

Informationen zum Definieren von Parametern für die IPQoS-Metermodule finden Sie unter „So planen Sie die Verkehrssteuerung" auf Seite 852.

Marker (dscpmk und dlcosmk) – Übersicht

Im Diffserv-Modellen markiert der *Marker* ein Paket mit einem Wert, der das Weiterleitungsverhalten widerspiegelt. *Markierung* ist der Prozess, einen Wert in den Paket-Header einzufügen, um so festzulegen, wie das Paket zum Netzwerk weitergeleitet wird. IPQoS enthält zwei Markermodule:

- `dscpmk` – Markiert das DS-Feld in einem IP-Paket-Header mit einem numerischen Wert, der als *Differentiated Services Codepoint* oder *DSCP* bezeichnet wird. Ein Diffserv-konformer Router kann den DS-Codepoint nutzen, um das geeignete Weiterleitungsverhalten für das Paket anzuwenden.
- `dlcosmk` – Markiert das virtuelle lokale Netzwerk (VLAN)-Tag eines Ethernet-Frameheaders mit einem numerischen Wert, der als *Benutzerpriorität* bezeichnet wird. Die Benutzerpriorität gibt die *Serviceklasse (Class of Service, CoS)* an, die das geeignete Weiterleitungsverhalten für das Datagramm definiert.

`dlcosmk` ist eine IPQoS-Ergänzung, die nicht zu dem von der IETF entworfenen Diffserv-Modell gehört.

Informationen zur Umsetzung einer Marker-Strategie für die QoS-Richtlinie finden Sie unter „So planen Sie das Weiterleitungsverhalten" auf Seite 855.

Flow Accounting (`flowacct`) – Übersicht

IPQoS fügt das `flowacct`-Accounting-Modul zum Diffserv-Modell hinzu. Mit `flowacct` können Sie Statistiken zum Verkehrswert erfassen und Kundenrechnungen in Übereinstimmung mit deren SLAs erstellen. Flow Accounting eignet sich darüber hinaus zur Kapazitätsplanung und Systemüberwachung.

Das `flowacct`-Modul arbeitet mit dem `acctadm` -Befehl, um eine Accounting-Protokolldatei zu erstellen. Das allgemeine Protokoll umfasst das IPQoS 5-Tuple sowie zwei zusätzliche Attribute, die in der folgenden Liste aufgeführt sind:

- Quelladresse
- Ursprungs-Port
- Zieladresse
- Ziel-Port
- Protokollnummer
- Anzahl der Pakete
- Anzahl der Byte

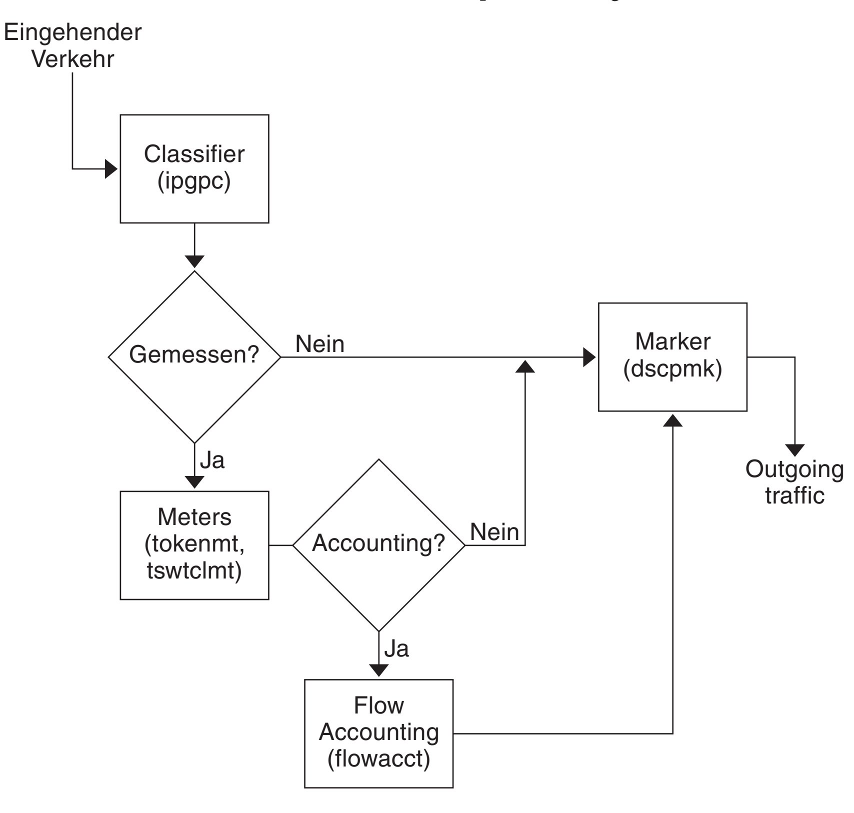
Darüber hinaus können Sie Statistiken zu anderen Attributen sammeln. Dies wird unter „Aufzeichnen von Informationen zu Verkehrswerten" auf Seite 902 und in den Manpages `flowacct`(7ipp) und `acctadm`(1M) beschrieben.

Informationen zur Planung einer Flow Accounting-Strategie finden Sie unter „So planen Sie das Flow Accounting" auf Seite 858.

So durchläuft ein Verkehrswert die IPQoS-Module

In der folgenden Abbildung wird ein Pfad gezeigt, den eingehender Datenverkehr über einige der IPQoS-Module nehmen könnte.

ABBILDUNG 32–1 Verkehrswert über eine IPQoS-Implementierung des Diffserv-Modells



Diese Abbildung zeigt eine allgemeine Verkehrswert-Sequenz auf einem IPQoS-konformen Computer:

1. Der Classifier wählt alle Pakete aus dem Paketstrom aus, die den Filterkriterien in der QoS-Richtlinie des Systems entsprechen.
2. Die ausgewählten Pakete werden dann ausgewertet, um die nächste auszuführende Aktion auszuwählen.
3. Der Classifier sendet jeglichen Verkehr, der keine Verkehrssteuerung benötigt, an den Marker.
4. Datenverkehr, für den eine Verkehrssteuerung erforderlich ist, wird an den Meter gesendet.
5. Der Meter setzt die konfigurierte Rate durch. Dann weist der Meter einen Verkehr-Konformitätswert für die flusskontrollierten Pakete zu.
6. Die flusskontrollierten Pakete werden daraufhin ausgewertet, um festzustellen, für welche Pakete ein Accounting erforderlich ist.
7. Der Meter sendet jeden Verkehr, für den kein Flow Accounting erforderlich ist, an den Marker.

8. Das Flow Accounting-Modul sammelt Statistiken zu den empfangenen Paketen. Dann sendet das Modul die Pakete an den Marker.
9. Der Marker weist dem Paket-Header einen DS Codepoint zu. Dieser DSCP kennzeichnet das Per-Hop-Behaviour, das ein Diffserv-konformes System an dem Paket anwenden muss.

Verkehrsweiterleitung in einem IPQoS-konformen Netzwerk

In diesem Abschnitt werden Sie in die Elemente eingeführt, die an der Weiterleitung von Paketen in einem IPQoS-konformen Netzwerk beteiligt sind. Ein IPQoS-konformes System verarbeitet beliebige Pakete in einem Netzwerk-Stream, die an die IP-Adresse des Systems gerichtet sind. Dann wendet das IPQoS-System seine QoS-Richtlinie an dem Paket an, um die Differentiated Services einzurichten.

DS Codepoint

Der DS Codepoint (DSCP) definiert die Aktion im Paket-Header, die ein Diffserv-konformes System an einem markierten Paket vornehmen soll. Die Diffserv-Architektur definiert eine Reihe von DS Codepoints für das IPQoS-konforme System sowie den zu verwendenden Diffserv-Router. Darüber hinaus definiert die Diffserv-Architektur eine Reihe von Aktionen, die als das *Weiterleitungsverhalten* bezeichnet werden. Dieses Weiterleitungsverhalten entspricht den DSCPs. Das IPQoS-konforme System markiert die Prioritätsstufenbits des DS-Felds im Paket-Header mit den DSCP. Empfängt ein Router ein Paket mit einem DSCP-Wert, wendet der Router das dem DSCP zugeordnete Weiterleitungsverhalten an. Anschließend wird das Paket für das Netzwerk freigegeben.

Hinweis – Der `dlcosmk`-Marker verwendet keine DSCP. Stattdessen markiert `dlcosmk` die Ethernet-Frameheader mit einem CoS-Wert. Wenn Sie beabsichtigen, IPQoS in einem Netzwerk zu konfigurieren, das VLAN-Geräte verwendet, lesen Sie „Markermodul“ auf Seite 913.

Per-Hop-Behaviors

In der Diffserv-Terminologie wird das einem DSCP zugeordnete Weiterleitungsverhalten als *Per-Hop-Behavior (PHB)* bezeichnet. Das PHB definiert die Prioritätsstufe der Weiterleitung, die ein markiertes Paket in Relation zu anderem Datenverkehr in einem Diffserv-konformen Systemen empfängt. Diese Prioritätsstufe legt maßgeblich fest, ob das IPQoS-konforme System oder der Diffserv-Router das markierte Paket weiterleitet oder abwirft. Bei einem weitergeleiteten Paket wendet jeder Diffserv-Router auf der Route des Pakets zu seinem Ziel das gleiche PHB an. Eine Ausnahme ist, wenn ein anderes Diffserv-System den DSCP ändert. Weitere Informationen zu PHBs finden Sie unter „Verwenden des Markers `dscpmk` zum Weiterleiten von Paketen“ auf Seite 913.

Das Ziel eines PHB besteht darin, einen bestimmten Teil an Netzwerkressourcen für eine Verkehrsklasse im angrenzenden Netzwerk bereitzustellen. Dieses Ziel erreichen Sie mit der QoS-Richtlinie. Definieren Sie DSCPs, die die Prioritätsstufen für Verkehrsklassen kennzeichnen, wenn Verkehrswerte das IPQoS-konforme System verlassen. Prioritätsstufen können im Bereich von einer high/low-drop-Wahrscheinlichkeit bis zu einer low/high-drop-Wahrscheinlichkeit definiert werden.

Beispielsweise kann Ihre QoS-Richtlinie einer Verkehrsklasse einen DSCP zuweisen, der ein low-drop PHB garantiert. Diese Verkehrsklasse erhält dann ein low-drop PHB von jedem Diffserv-konformen Router, der Paketen dieser Klasse Bandbreite garantiert. Sie können die QoS-Richtlinie anderen DSCPs hinzufügen, die anderen Verkehrsklassen wechselnde Prioritätsstufen zuweisen. Paketen mit geringerer Prioritätsstufe erhalten von den Diffserv-Systemen Bandbreite gemäß den Prioritäten, die in den DSCPs der Pakete angegeben sind.

IPQoS unterstützt zwei Arten von Weiterleitungsverhalten, die in der Diffserv-Architektur definiert sind: Expedited Forwarding und Assured Forwarding.

Expedited Forwarding

Das *Expedited Forwarding (EF)* Per-Hop-Behavior stellt sicher, dass eine Verkehrsklasse mit EFs-bezogenem DSCP die höchste Priorität erhält. Verkehr mit einem EF DSCP wird nicht in eine Warteschlange gestellt. EF bietet geringen Verlust, Latenzzeit und Jitter. Der empfohlene DSCP für EF ist 101110. Ein Paket, das mit 101110 markiert ist, erhält eine garantierte low-drop-Prioritätsstufe, wenn das Paket auf der Route zum Ziel auf Diffserv-konforme Netzwerke trifft. Verwenden Sie das EF DSCP, wenn Sie Kunden oder Anwendungen mit einem Premium-SLA Priorität zuweisen.

Assured Forwarding

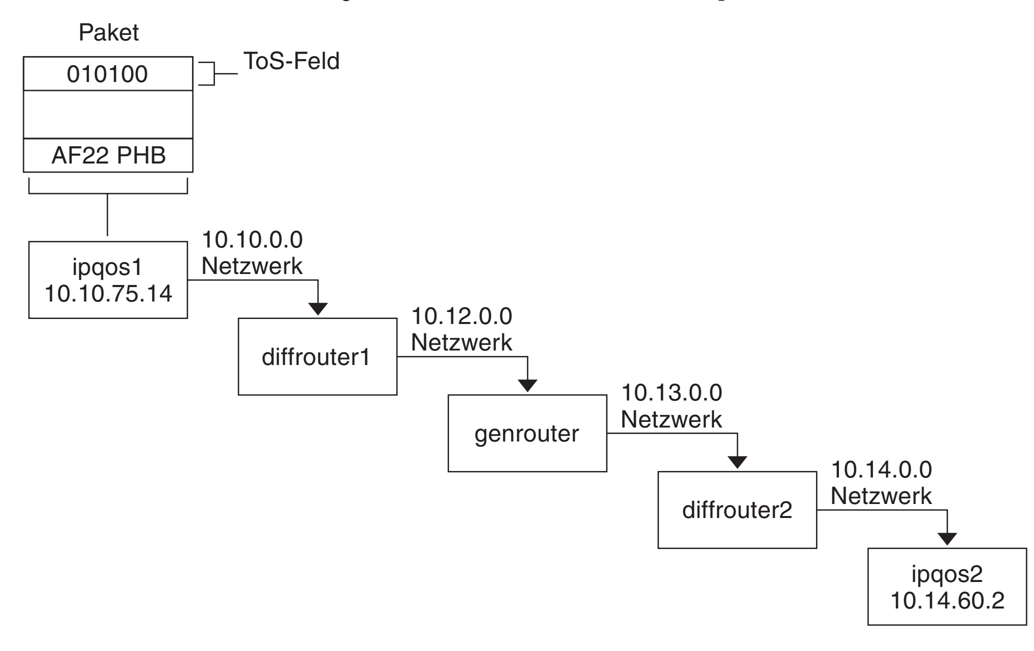
Das *Assured Forwarding (AF)* Per-Hop-Behavior bietet vier unterschiedliche Weiterleitungsklassen, die Sie einem Paket zuweisen können. Jede Weiterleitungsklasse bietet drei drop-Prioritätsstufen, die in Tabelle 37–2 aufgeführt sind.

Die verschiedenen AF Codepoints bieten die Möglichkeit, Kunden und Anwendungen unterschiedliche Serviceebenen zuzuweisen. In der QoS-Richtlinie können Sie schon bei der Planung Verkehr und Services in Ihren Netzwerk priorisieren. Dann können Sie dem priorisierten Verkehr unterschiedliche AF-Ebenen zuweisen.

Paketweiterleitung in einer Diffserv-Umgebung

Die folgende Abbildung zeigt einen Teil eines Unternehmens-Intranets mit einer teilweise Diffserv-konformen Umgebung. In diesem Szenario sind alle Hosts in den Netzwerken `10.10.0.0` und `10.14.0.0` IPQoS-konform und die lokalen Router in beiden Netzwerken sind Diffserv-konform. Jedoch sind die Zwischennetzwerke nicht für Diffserv konfiguriert.

ABBILDUNG 32–2 Paketweiterleitung über Diffserv-konforme Netzwerk-Hops



Die nächsten Schritte verfolgen den Verlauf des in der Abbildung gezeigten Pakets. Die Schritte beginnen mit dem Fortschritt eines Pakets, das seinen Ursprung bei Host `ipqos1` hat. Die nächsten Schritte beschreiben den weiteren Verlauf über mehrere Hops zum Host `ipqos2`.

1. Der Benutzer an `ipqos1` führt den Befehl `ftp` aus, um auf Host `ipqos2` zuzugreifen, der drei Hops entfernt ist.
2. `ipqos1` wendet seine QoS-Richtlinie an dem resultierenden Datenpaketstrom an. `ipqos1` klassifiziert daraufhin erfolgreich den `ftp`-Verkehr.

   Der Systemadministrator hat eine Klasse für den gesamten abgehenden `ftp`-Verkehr erstellt, der seinen Ursprung im lokalen Netzwerk 10.10.0.0 hat. Verkehr für die `ftp`-Klasse wird das AF22 Per-Hop-Behavior zugewiesen: Klasse zwei, medium-drop-Prioritätsstufe. Für die `ftp`-Klasse ist eine Verkehrswertrate von 2Mbit/s konfiguriert.
3. `ipqos-1` misst den `ftp`-Datenfluss, um festzustellen, ob der Fluss die zulässige Rate von 2 Mbit/s überschreitet.
4. Der Marker auf `ipqos1` markiert die DS-Felder in den abgehenden `ftp`-Paketen mit dem 010100 DSCP, entsprechend dem AF22 PHB.
5. Der Router `diffrouter1` empfängt die `ftp`-Pakete. `diffrouter1` prüft den DSCP. Wenn `diffrouter1` überlastet ist, werden Pakete, die mit AF22 markiert sind, abgeworfen.
6. `ftp`-Verkehr wird in Übereinstimmung mit dem Per-Hop-Behavior, das für AF22 in den `diffrouter1`-Dateien konfiguriert ist, an den nächsten Hop weitergeleitet.

7. Der `ftp`-Verkehr durchläuft das Netzwerk `10.12.0.0` zum `genrouter`, der nicht Diffserv-konform ist. Hier erhält der Verkehr ein „Beste Leistung"-Weiterleitungsverhalten.
8. `genrouter` übergibt den `ftp`-Verkehr an das Netzwerk `10.13.0.0`. Hier wird er von `diffrouter2` empfangen.
9. `diffrouter2` ist Diffserv-konform. Aus diesem Grund leitet der Router die `ftp`-Pakete in Übereinstimmung mit dem PHB, das in der Router-Richtlinie für AF22-Pakete definiert ist, an das Netzwerk weiter.
10. `ipqos2` empfängt den `ftp`-Verkehr. `ipqos2` fordert als Nächstes den Benutzer an `ipqos1` zur Eingabe von Benutzernamen und Passwort auf.

KAPITEL 33

Planen eines IPQoS-konformen Netzwerks (Aufgaben)

Sie können IPQoS auf jedem System konfigurieren, auf dem Oracle Solaris ausgeführt wird. Das IPQoS-System arbeitet dann mit Diffserv-konformen Routern, um Differentiated Services und Verkehrsmanagement in einem Intranet bereitzustellen.

In diesem Kapitel sind die Planungsaufgaben zum Hinzufügen von IPQoS-konformen Systemen zu einem Diffserv-konformen Netzwerk aufgeführt. In diesem Kapitel werden folgende Themen behandelt.

- „Planen einer allgemeinen IPQoS-Konfiguration (Übersicht der Schritte)" auf Seite 841
- „Planen der Diffserv-Netzwerktopologie" auf Seite 842
- „Planen der Quality of Service-Richtlinie" auf Seite 845
- „Planen einer QoS-Richtlinie (Übersicht der Schritte)" auf Seite 846
- „Einführung in das IPQoS-Konfigurationsbeispiel" auf Seite 859

Planen einer allgemeinen IPQoS-Konfiguration (Übersicht der Schritte)

Das Umsetzen von Differentiated Services, einschließlich IPQoS, in einem Netzwerk erfordert umfangreiche Planung. Sie müssen nicht nur Position und Funktion aller IPQoS-konformen Systemen berücksichtigen, sondern auch die Beziehung jedes Systems zum Router im lokalen Netzwerk. In der folgenden Tabelle sind die wichtigsten Planungsaufgaben für die Implementierung von IPQoS in Ihrem Netzwerk sowie Links zu Verfahren zur Durchführung der Aufgaben aufgeführt.

Aufgabe	Beschreibung	Siehe
1. Planen einer Diffserv-Netzwerktopologie, die IPQoS-konforme Systeme enthält.	Lernen Sie die verschiedenen Diffserv-Netzwerktopologien kennen, um die beste Lösung für Ihren Standort zu ermitteln.	„Planen der Diffserv-Netzwerktopologie" auf Seite 842.

Aufgabe	Beschreibung	Siehe
2. Planen der verschiedenen Servicetypen, die von den IPQoS-Systemen bereitgestellt werden sollen.	Strukturieren Sie die Servicetypen, die das Netzwerk anbieten soll, in Service-Level Agreements (SLAs).	„Planen der Quality of Service-Richtlinie" auf Seite 845.
3. Planen der QoS-Richtlinie für jedes IPQoS-System.	Treffen Sie Entscheidungen hinsichtlich der Klassen und der Meter- und Accounting-Funktionen, die zur Umsetzung jeder SLA erforderlich sind.	„Planen der Quality of Service-Richtlinie" auf Seite 845.
4. Wenn anwendbar, planen der Richtlinie für den Diffserv-Router.	Treffen Sie Entscheidungen zu den Scheduling- und Queuing-Richtlinien für den Diffserv-Router, die mit den IPQoS-Systemen verwendet werden.	Informationen zu den Queuing- und Scheduling-Richtlinien entnehmen Sie der Router-Dokumentation.

Planen der Diffserv-Netzwerktopologie

Um in Ihrem Netzwerk Differentiated Services bereitstellen zu können, müssen Sie mindestens ein IPQoS-konformes System und einen Diffserv-konformen Router konfigurieren. Sie können dieses Basisszenario auf verschiedene Arten erweitern. Informationen hierzu finden Sie in diesem Abschnitt.

Hardware-Strategien für das Diffserv-Netzwerk

In der Regel führen Kunden IPQoS auf Servern und Server-Konsolidierungen, z. B. dem Sun Enterprise™ 0000-Server aus. Umgekehrt können Sie IPQoS abhängig von den Anforderungen Ihres Netzwerks auf Desktopsystemen wie UltraSPARC®-Systemen ausführen. In der folgenden Liste sind mögliche Systeme für eine IPQoS-Konfiguration aufgeführt:

- Oracle Solaris-Systeme, die verschiedene Services anbieten, z. B. Webserver und Datenbankserver
- Anwendungsserver, die E-Mail, FTP und andere beliebte Netzwerkanwendungen anbieten
- Web-Cache-Server oder Proxy-Server
- Ein Netzwerk mit IPQoS-konformen Serverfarmen, die von Diffserv-konformen Load-Balancers verwaltet werden
- Netzwerke, die Datenverkehr für ein einzelnes heterogenes Netzwerk verwalten
- IPQoS-Systeme, die Teil eines virtuellen lokalen Netzwerkes (LAN) sind

Sie können IPQoS-Systeme auch in eine Netzwerktopologie mit bereits ordnungsgemäß arbeitenden Diffserv-konformen Routern einführen. Falls Ihr Router derzeit keine Diffserv anbietet, sollten Sie den Einsatz von Diffserv-Lösungen in Betracht ziehen, die von Cisco Systems, Juniper Networks und anderen Router-Herstellern angeboten werden. Wenn Ihr lokaler Router keine Diffserv implementiert, übergibt der Router markierte Pakete an den nächsten Hop, ohne die Marker auszuwerten.

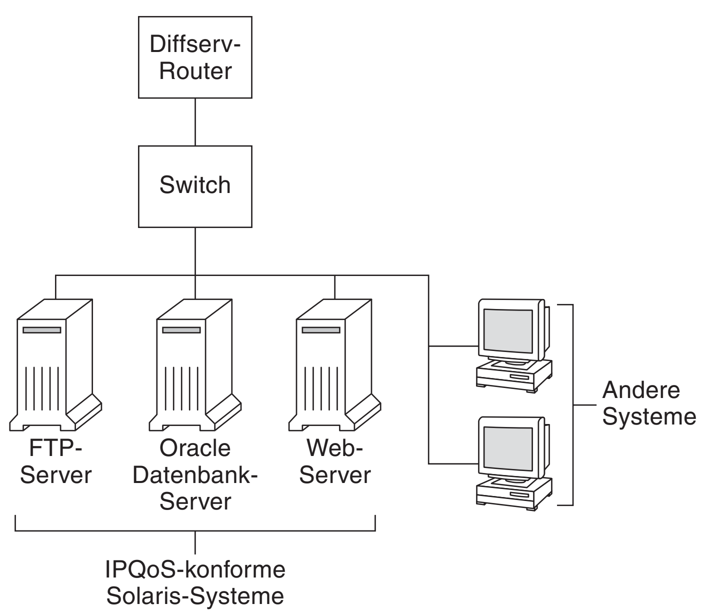
IPQoS-Netzwerktopologien

Dieser Abschnitt zeigt IPQoS-Strategien für verschiedene Netzwerkanforderungen.

IPQoS auf einzelnen Hosts

Die folgende Abbildung zeigt ein einzelnes Netzwerk mit IPQoS-konformen Systemen.

ABBILDUNG 33–1 IPQoS-Systeme in einem Netzwerksegment



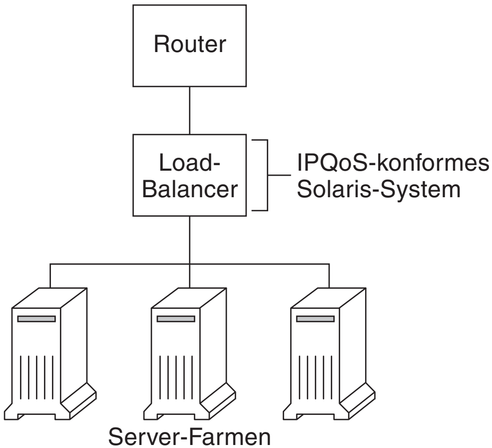
Dieses Netzwerk ist ein Segment eines Unternehmens-Intranets. Durch Aktivieren von IPQoS auf den Anwendungsservern und Webservern können Sie die Rate kontrollieren, mit der jedes IPQoS-System abgehenden Verkehr freigibt. Wenn Sie den Router Diffserv-konform konfigurieren, können Sie eingehenden und abgehenden Verkehr weiter kontrollieren.

Die Beispiele in diesem Handbuch basieren auf dem Szenario „IPQoS auf einem einzelnen Host“. Die in diesem Handbuch verwendete Beispieltopologie finden Sie in Abbildung 33–4.

IPQoS in einem Netzwerk aus Serverfarmen

Die folgende Abbildung zeigt ein Netzwerk mit mehreren heterogenen Serverfarmen.

ABBILDUNG 33–2 Netzwerk mit IPQoS-konformen Serverfarmen



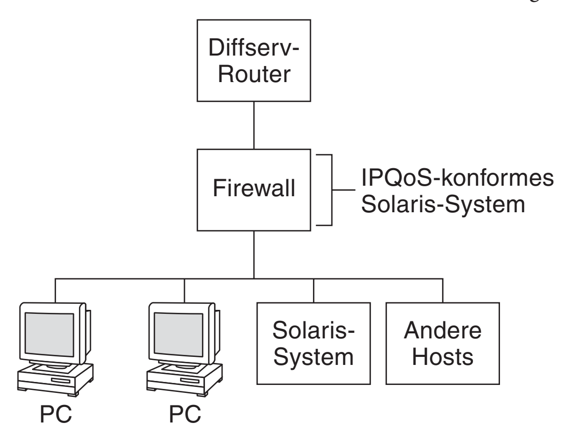
In einer solchen Topologie ist der Router Diffserv-konform und somit in der Lage, sowohl eingehenden als auch abgehenden Verkehr in eine Warteschlange zu stellen und zu berechnen. Auch der Load-Balancer ist Diffserv-konform und die Serverfarmen sind IPQoS-konform. Der Load-Balancer kann mithilfe von Selektoren wie der Benutzer-ID und der Projekt-ID zusätzliche Filteraufgaben über den Router hinaus wahrnehmen. Diese Selektoren sind in den Anwendungsdaten enthalten.

Dieses Szenario bietet Verkehrssteuerung und -weiterleitung, um Überlastungen im lokalen Netzwerk zu vermeiden. Darüber hinaus verhindert dieses Szenario, das von den Serverfarmen abgehender Verkehr andere Teile des Intranets überlastet.

IPQoS und Firewalls

Die folgende Abbildung zeigt ein Segment eines Unternehmensnetzwerks, das von anderen Segmenten wird durch eine Firewall gesichert ist.

ABBILDUNG 33–3 Durch eine IPQoS-konforme Firewall geschütztes Netzwerk



In diesem Szenario trifft der Verkehrswert bei einem Diffserv-konformen Router an, der die Pakete filtert und in eine Warteschlange stellt. Der gesamte eingehende Verkehr, der über den Router weitergeleitet wird, durchläuft eine IPQoS-konforme Firewall. Um IPQoS zu verwenden, darf die Firewall den IP-Weiterleitungsstapel nicht umgehen.

Die Sicherheitsrichtlinie der Firewall legt fest, ob eingehender Verkehr in das interne Netzwerk eintreten oder es verlassen darf. Die QoS-Richtlinie kontrolliert die Serviceebenen für eingehenden Verkehr, der die Firewall passiert hat. Abhängig von der QoS-Richtlinie kann abgehender Verkehr ebenfalls mit einem Weiterleitungsverhalten versehen werden.

Planen der Quality of Service-Richtlinie

Wenn Sie die Quality of Service (QoS)-Richtlinie planen, müssen Sie die von Ihrem Netzwerk angebotenen Services prüfen, klassifizieren und priorisieren. Außerdem müssen Sie die verfügbare Bandbreite bewerten, um die Rate festzulegen, mit der jede Verkehrsklasse im Netzwerk freigegeben wird.

Hilfen bei der Planung einer QoS-Richtlinie

Sammeln Sie Informationen zur Planung der QoS-Richtlinie in einem Format, das die Informationen umfasst, die für die IPQoS-Konfigurationsdatei erforderlich sind. Verwenden Sie beispielsweise die folgende Vorlage, um die wichtigsten der in der IPQoS-Konfigurationsdatei verwendeten Informationskategorien aufzulisten.

TABELLE 33–1 Vorlage zur Planung einer QoS-Richtlinie

Klasse	Priorität	Filter	Selektor	Rate	Weiterleitung?	Accounting?
Klasse 1	1	Filter 1 Filter 3	Selektor 1 Selektor 2	Meterraten, abhängig vom Metertyp	Marker drop-Prioritätsstufe	Erfordert Flow Accounting-Statistiken
Klasse 1	1	Filter 2	Selektor 1 Selektor 2	entf.	entf.	entf.
Klasse 2	2	Filter 1	Selektor 1 Selektor 2	Meterraten, abhängig vom Metertyp	Marker drop-Prioritätsstufe	Erfordert Flow Accounting-Statistiken
Klasse 2	2	Filter 2	Selektor 1 Selektor 2	entf.	entf.	entf.

Sie können jede Hauptkategorie weiter unterteilen, um die QoS-Richtlinie genauer zu definieren. In den nachfolgenden Abschnitten wird beschrieben, wie Sie die Informationen für die in der Vorlage beschriebenen Kategorien beziehen.

Planen einer QoS-Richtlinie (Übersicht der Schritte)

In der folgenden Tabelle sind die wichtigsten Aufgaben zur Planung einer QoS-Richtlinie sowie Links zu den Anleitungen zur Durchführung der einzelnen Aufgaben aufgeführt.

Aufgabe	Beschreibung	Siehe
1. Entwerfen Ihrer Netzwerktopologie zur Unterstützung von IPQoS.	Identifizieren Sie die Hosts und Router in Ihrem Netzwerk, um Differentiated Services bereitzustellen.	„So bereiten Sie ein Netzwerk für IPQoS vor“ auf Seite 847
2. Definieren der Klassen, in die die Services in Ihrem Netzwerk aufgeteilt werden.	Prüfen Sie die von Ihrem Standort angebotenen Servicetypen und SLAs, und legen Sie die einzelnen Verkehrsklassen fest, in die diese Services fallen.	„So definieren Sie die Klassen für Ihre QoS-Richtlinie“ auf Seite 848
3. Definieren der Filter für die Klassen.	Ermitteln Sie die am besten geeigneten Möglichkeiten zum Trennen von Datenverkehr einer bestimmten Klasse vom Netzwerk-Verkehrswert.	„So definieren Sie Filter in der QoS-Richtlinie“ auf Seite 851

Aufgabe	Beschreibung	Siehe
4. Definieren von Datenfluss-Steuerungsraten zur Messung von Verkehr, während Pakete das IPQoS-System verlassen.	Legen Sie akzeptable Datenflussraten für jede Verkehrsklasse fest.	„So planen Sie die Verkehrssteuerung“ auf Seite 852
5. Definieren der DSCPs oder Benutzerpriorität-Werte, die in der QoS-Richtlinie verwendet werden.	Planen Sie ein Schema, um das Weiterleitungsverhalten festzulegen, das einem Verkehrswert zugeordnet wird, wenn der Fluss von einem Router oder einem Switch verarbeitet wird.	„So planen Sie das Weiterleitungsverhalten“ auf Seite 855
6. Wenn anwendbar, Einrichten eines Plans zur Überwachung der Statistiken für die Verkehrswerte im Netzwerk.	Werten Sie die Verkehrsklassen aus, um festzustellen, welche Verkehrswerte für Accounting- oder statistische Zwecke überwacht werden müssen.	„So planen Sie das Flow Accounting“ auf Seite 858

Hinweis – Im weiteren Verlauf dieses Abschnitts wird erklärt, wie Sie die QoS-Richtlinie eines IPQoS-konformen Systems planen. Informationen zur Planung der QoS-Richtlinie für den Diffserv-Router entnehmen Sie bitte der Router-Dokumentation und der Website des Router-Herstellers.

▼ So bereiten Sie ein Netzwerk für IPQoS vor

Im folgenden Verfahren sind die allgemeinen Planungsaufgaben zum Erstellen der QoS-Richtlinie beschrieben.

1. **Erstellen Sie eine Übersicht Ihrer Netzwerktopologie. Dann planen Sie eine Strategie, die IPQoS-Systeme und Diffserv-Router eingesetzt.**

   Topologiebeispiele finden Sie unter „Planen der Diffserv-Netzwerktopologie“ auf Seite 842.

2. **Kennzeichnen Sie die Hosts in der Topologie, die IPQoS erfordern oder sich für den IPQoS-Service eignen.**

3. **Stellen Sie fest, welche IPQoS-konformen Systemen die gleiche QoS-Richtlinie verwenden können.**

   Wenn Sie beabsichtigen, IPQoS auf allen Hosts im Netzwerk zu aktivieren, kennzeichnen Sie alle Hosts, die die gleiche QoS-Richtlinie verwenden können. Jedes IPQoS-konforme System muss über eine lokale QoS-Richtlinie verfügen, die in dessen IPQoS-Konfigurationsdatei implementiert ist. Sie können jedoch auch eine IPQoS-Konfigurationsdatei erstellen, die von mehreren Systemen verwendet wird. Dann kopieren Sie die Konfigurationsdatei auf jedes System mit dem gleichen Anforderungen an eine QoS-Richtlinie.

4 Erstellen Sie eine Übersicht aller Planungsaufgaben, die für den Diffserv-Router in Ihrem Netzwerk erforderlich sind, und führen Sie sie aus.

Einzelheiten entnehmen Sie bitte der Router-Dokumentation und der Website des Router-Herstellers.

▼ So definieren Sie die Klassen für Ihre QoS-Richtlinie

Der erste Schritt beim Definieren der QoS-Richtlinie ist das Strukturieren der Verkehrswerte in Klassen. Es ist nicht erforderlich, für jeden Verkehrstyp in einem Diffserv-Netzwerk eine Klasse zu erstellen. Darüber hinaus müssen Sie, abhängig von Ihrer Netzwerktopologie, eventuell für jedes IPQoS-konforme System eine andere QoS-Richtlinie erstellen.

Hinweis – Eine Übersicht der Klassen finden Sie unter „IPQoS-Klassen" auf Seite 832.

Für das nächste Verfahren wird davon ausgegangen, dass Sie festgelegt haben, welche Systeme in Ihrem Netzwerk IPQoS-konform sind. Informationen hierzu finden Sie unter „So bereiten Sie ein Netzwerk für IPQoS vor" auf Seite 847.

1 Erstellen Sie eine QoS-Planungstabelle zur Strukturierung der QoS-Richtlinieninformationen.

Vorschläge finden Sie in Tabelle 33–1.

2 Führen Sie die verbleibenden Schritte für jede QoS-Richtlinie in Ihrem Netzwerk aus.

3 Definieren Sie die in der QoS-Richtlinie zu verwendenden Klassen.

Die folgenden Fragen stellen eine Richtlinie zum Analysieren des Netzwerkverkehrs für mögliche Klassendefinitionen dar.

- **Bietet Ihr Unternehmen seinen Kunden Service-Level Agreements an?**

  In diesem Fall bewerten Sie die relativen Prioritätsebenen der SLAs, die Ihr Unternehmen seinen Kunden anbietet. Die gleichen Anwendungen können Kunden angeboten werden, denen unterschiedliche Prioritätsebenen garantiert sind.

  Angenommen, Ihr Unternehmen bietet jedem Kunden Website-Hosting an. Dies bedeutet, dass Sie für jede Kunden-Website eine Klasse definieren müssen. Eine SLA kann eine Premium-Website als eine Serviceebene bereitstellen. Eine andere SLA bietet eventuell eine „Beste Leistung" Personal-Website für Kunden zu einem Discountpreis an. Diese Faktoren deutet darauf hin, dass nicht nur unterschiedliche Websiteklassen, sondern diesen Websiteklassen auch potentiell unterschiedliche Per-Hop-Behaviors zugeordnet sind.

- **Bietet das IPQoS-Systemen populäre Anwendungen, die eine Verkehrssteuerung erfordern?**

Sie können die Netzwerkleistung verbessern, indem Sie IPQoS auf Servern aktivieren, die populäre Anwendungen bereitstellen, die hohen Netzverkehr erzeugen. Typische Beispiele sind E-Mail, Netzwerknachrichten und FTP. Ziehen Sie, sofern anwendbar, das Erstellen von separaten Klassen für eingehenden und abgehenden Verkehr für jeden Servicetyp in Betracht. Beispielsweise können Sie eine Klasse für `eingehende Mail` und eine Klasse für `abgehende Mail` für die QoS-Richtlinie eines Mailservers erstellen.

- **Führt Ihr Netzwerk bestimmte Anwendungen aus, die ein Weiterleitungsverhalten mit der höchsten Priorität erfordern?**

  Jede kritische Anwendung, die ein Weiterleitungsverhalten mit höchster Priorität erfordert, muss die höchste Priorität in der Router-Warteschlange erhalten. Typische Beispiele sind Streaming-Video und Streaming-Audio.

  Definieren Sie eingehende Klassen und abgehende Klassen für diese Anwendungen mit höchster Priorität. Dann fügen Sie die Klassen zu den QoS-Richtlinien auf dem IPQoS-konformen System, das als Server für die Anwendungen dient, sowie zum Diffserv-Router hinzu.

- **Treten in Ihrem Netzwerk Verkehrsströme auf, die gesteuert werden müssen, da sie einen Großteil der Bandbreite konsumieren?**

  Verwenden Sie `netstat`, `snoop` und andere Serviceprogramme zur Netzwerküberwachung, um Verkehr zu identifizieren, der zu Problemen im Netzwerk führen kann. Erstellen Sie eine Übersicht der bisher erstellten Klassen und erstellen Sie neue Klassen für eine Verkehrskategorie, die nicht näher definierte Probleme erzeugt. Wenn Sie bereits Klassen für eine Kategorie problembehafteten Verkehrs erzeugt haben, definieren Sie Raten für den Meter, mit denen der problembehaftete Verkehr kontrolliert wird.

  Erstellen Sie Klassen für den problembehafteten Verkehr auf jedem IPQoS-konformen Systemen im Netzwerk. Jedes IPQoS-System kann daraufhin problembehafteten Verkehr verarbeiten, indem es die Rate begrenzt, mit der der Verkehrswert in das Netzwerk freigegeben wird. Denken Sie daran, diese Problemklassen auch in der QoS-Richtlinie auf dem Diffserv-Router zu definieren. Der Router kann dann die problembehafteten Datenströme gemäß der Konfiguration in seiner QoS-Richtlinie in eine Warteschlange stellen und einplanen.

- **Müssen Sie Statistiken zu bestimmten Verkehrstypen beziehen?**

  Eine schnelle Überprüfung einer SLA bringt zum Vorschein, für welche Arten von Kundenverkehr Accounting erforderlich ist. Wenn Ihr Standort SLAs anbietet, haben Sie wahrscheinlich Klassen für den Verkehr erstellt, für den Accounting erforderlich ist. Darüber hinaus müssen Sie eventuell Klassen erstellen, um das Erfassen von Statistiken zu überwachten Verkehrswerten zu ermöglichen. Sie können auch Klassen für Verkehr erstellen, auf den der Zugriff aus Sicherheitsgründen eingeschränkt werden soll.

4. **Erstellen Sie eine Übersicht der von Ihnen definierten Klassen in der QoS-Planungstabelle, die Sie in Schritt 1 erstellt haben.**

5 **Weisen Sie jeder Klasse eine Prioritätsebene zu.**

Beispielsweise könnte Prioritätsebene 1 die höchste Prioritätsklasse darstellen. Weisen Sie den verbleibenden Klassen niedrigere Prioritätsebenen zu. Die von Ihnen zugewiesene Prioritätsebene dient nur zu organisatorischen Zwecken. Prioritätsebenen, die Sie in der QoS-Richtlinienvorlage aufstellen, werden nicht tatsächlich vom IPQoS verwendet. Darüber hinaus können Sie mehreren Klassen die gleiche Priorität zuweisen, falls dies für Ihre QoS-Richtlinie geeignet ist.

6 **Nachdem die Klassendefinition abgeschlossen ist, beginnen Sie mit der Definition von Filtern für jede Klasse. Dies ist unter „So definieren Sie Filter in der QoS-Richtlinie" auf Seite 851 beschrieben.**

Weitere Informationen: Priorisieren der Klassen

Beim Erstellen von Klassen werden Sie schnell feststellen, welche Klassen die höchste Priorität, eine mittlere Priorität und eine „Beste Leistung"-Priorität erhalten sollen. Ein gut geeignetes Schema zur Priorisierung von Klassen wird insbesondere dann wichtig, wenn Sie abgehenden Verkehr ein Per-Hop-Behavior zuweisen. Dies wird unter „So planen Sie das Weiterleitungsverhalten" auf Seite 855 beschrieben.

Neben dem Zuweisen eines PHB zu einer Klasse können Sie auch einen Prioritätsselektor in einem Filter für die Klasse definieren. Der Prioritätsselektor ist nur auf dem IPQoS-konformen Host aktiv. Angenommen, einige Klassen mit gleichen Raten und identischen DSCPs stehen beim Verlassen des IPQoS-Systems im Wettbewerb um Bandbreite. Der Prioritätsselektor in jeder Klasse kann die Serviceebene anderweitig identisch bewerteter Klassen weiter aufschlüsseln.

Definieren von Filtern

Sie erstellen Filter, um die Mitgliedschaft des Paketflusses bei einer bestimmten Klasse zu identifizieren. Jeder Filter enthält Selektoren, die Kriterien zur Bewertung eines Paketflusses definieren. Das IPQoS-konforme System verwendet die Kriterien in den Selektoren, um Pakete aus einem Verkehrswert zu extrahieren. Dann weist das IPQoS-System die Pakete einer Klasse zu. Eine Einführung in das Konzept der Filter finden Sie unter „IPQoS-Filter" auf Seite 832.

In der folgenden Tabelle sind die am häufigsten verwendeten Selektoren aufgeführt. Die ersten fünf Selektoren stellen das IPQoS 5-Tuple dar, das vom IPQoS-System verwendet wird, um Pakete als Mitglieder eines Datenflusses zu identifizieren. Eine vollständige Liste der Selektoren finden Sie in Tabelle 37–1.

TABELLE 33–2 Allgemeine IPQoS-Selektoren

Name	Definition
saddr	Quelladresse.
daddr	Zieladresse.
sport	Ursprungs-Portnummer. Sie können eine bekannte Portnummer gemäß der Definition in /etc/services oder eine benutzerdefinierte Portnummer verwenden.
dport	Ziel-Portnummer.
protocol	IP-Protokollnummer oder Protokollname, der dem Verkehrswerttyp in /etc/protocols zugewiesen ist.
ip_version	Zu verwendender Adressierungstyp. Verwenden Sie entweder IPv4 oder IPv6. IPv4 ist die Standardeinstellung.
dsfield	Inhalt des DS-Felds, das heißt, der DSCP. Verwenden Sie diesen Selektor zum Extrahieren eingehender Pakete, die bereits mit einem bestimmten DSCP markiert sind.
priority	Prioritätsebene, die der Klasse zugewiesen ist. Weitere Informationen finden Sie unter „So definieren Sie die Klassen für Ihre QoS-Richtlinie“ auf Seite 848.
user	Entweder die UNIX-Benutzer-ID oder der Benutzername, der beim Ausführen der Anwendung auf höherer Ebene verwendet wird.
projid	Projekt-ID, die beim Ausführen der Anwendung auf höherer Ebene verwendet wird.
direction	Die Richtung des Verkehrswerts. Gültige Werte sind entweder LOCAL_IN, LOCAL_OUT, FWD_IN oder FWD_OUT.

Hinweis – Selektoren sollten nur nach sorgfältigen Überlegungen zugewiesen werden. Verwenden Sie nur so viele Selektoren, wie Sie zum Extrahieren der Pakete für eine Klasse benötigen. Je mehr Selektoren Sie definieren, desto größer sind die Auswirkungen auf die IPQoS-Performance.

▼ So definieren Sie Filter in der QoS-Richtlinie

Bevor Sie beginnen Bevor Sie die nächsten Schritte ausführen, sollten Sie das Verfahren „So definieren Sie die Klassen für Ihre QoS-Richtlinie“ auf Seite 848 vollständig abgeschlossen haben.

1 Definieren Sie mindestens einen Filter für jede Klasse in der QoS-Planungstabelle, die Sie unter „So definieren Sie die Klassen für Ihre QoS-Richtlinie" auf Seite 848 erstellt haben.

Denken Sie daran, sofern anwendbar, separate Filter für eingehende und abgehenden Verkehr für jede Klasse zu erstellen. Fügen Sie beispielsweise einen Filter für `ftp-in` und einen Filter für `ftp-out` in die QoS-Richtlinie eines IPQ-konformen FTP-Servers ein. Dann können Sie zusätzlich zu den allgemeinen Selektoren einen geeigneten `direction`-Selektor definieren.

2 Definieren Sie mindestens einen Selektor für jeden Filter in einer Klasse.

Verwenden Sie die in Tabelle 33–1 eingeführte QoS-Planungstabelle, um Filter für die von Ihnen definierten Klassen einzufügen.

Beispiel 33–1 Definieren von Filtern für FTP-Verkehr

In der folgenden Tabelle, die als Beispiel dient, wird gezeigt, wie Sie einen Filter für abgehenden FTP-Verkehr definieren.

Klasse	Priorität	Filter	Selektoren
`ftp-traffic`	4	`ftp-out`	`saddr 10.190.17.44`
			`daddr 10.100.10.53`
			`sport 21`
			`direction LOCAL_OUT`

Siehe auch

- Informationen zum Definieren eines Schemas für die Flusskontrolle finden Sie unter „So planen Sie die Verkehrssteuerung" auf Seite 852.
- Informationen zum Definieren des Weiterleitungsverhaltens für Datenströme, die zum Netzwerkstrom zurückkehren, finden Sie unter „So planen Sie das Weiterleitungsverhalten" auf Seite 855.
- Informationen zum Planen des Flow Accounting für bestimmte Arten von Datenverkehr finden Sie unter „So planen Sie das Flow Accounting" auf Seite 858.
- Informationen zum Hinzufügen weiterer Klassen zur QoS-Richtlinie finden Sie unter „So definieren Sie die Klassen für Ihre QoS-Richtlinie" auf Seite 848.
- Informationen zum Hinzufügen weiterer Filter zur QoS-Richtlinie finden Sie unter „So definieren Sie Filter in der QoS-Richtlinie" auf Seite 851.

▼ So planen Sie die Verkehrssteuerung

Die Verkehrssteuerung umfasst das Messen des Verkehrswerts für eine Klasse sowie das Freigeben der Pakete mit einer definierten Rate in das Netzwerk. Beim Planen einer Verkehrssteuerung definieren Sie die Parameter, die von den IPQoS-Metermodule verwendet

werden sollen. Die Metermodule bestimmen die Rate, mit der Verkehr in das Netzwerk freigegeben wird. Eine Einführung in das Konzept der Metermodule finden Sie unter „Meter (`tokenmt` und `tswtclmt`) – Übersicht“ auf Seite 833.

Im folgenden Verfahren wird davon ausgegangen, dass Sie Filter und Selektoren bereits definiert haben. Dies wird unter „So definieren Sie Filter in der QoS-Richtlinie“ auf Seite 851 beschrieben.

1. **Ermitteln Sie die maximale Bandbreite Ihres Netzwerks.**

2. **Erstellen Sie eine Übersicht aller SLAs, die von Ihrem Netzwerk unterstützt werden. Identifizieren Sie die Kunden und den Servicetyp, der jedem Kunden garantiert ist.**

   Um eine bestimmte Serviceebene zu garantieren, müssen Sie die vom Kunden erzeugten bestimmten Verkehrsklassen messen.

3. **Erstellen Sie eine Übersicht der Klassen, die Sie unter „So definieren Sie die Klassen für Ihre QoS-Richtlinie“ auf Seite 848 erstellt haben.**

   Stellen Sie fest, ob weitere Klassen außer den SLAs zugewiesenen Klassen gemessen werden müssen.

   Angenommen, das IPQoS-System führt eine Anwendung aus, die starken Datenverkehr erzeugt. Nachdem Sie den Verkehr der Anwendung klassifiziert haben, messen Sie die Datenströme, um die Rate zu steuern, mit der die Pakete des Datenflusses in das Netzwerk zurückkehren.

Hinweis – Nicht alle Klassen müssen gemessen werden. Beachten Sie dies beim Erstellen einer Übersicht Ihrer Klassen.

---

4. **Ermitteln Sie, welche Filter in jeder Klasse den Datenverkehr auswählen, für den eine Verkehrssteuerung erforderlich ist. Dann passen Sie die Liste der Klassen an, für die eine Messung erforderlich ist.**

   Klassen mit mehreren Filtern erfordern eventuell nur Messungen für einen Filter. Angenommen, Sie definieren Filter für eingehenden und abgehenden Datenverkehr einer bestimmten Klasse. Dann stellen Sie fest, dass die Verkehrssteuerung nur für den Datenverkehr in eine Richtung erforderlich ist.

5. **Wählen Sie ein Metermodul für jede Klasse, für die eine Verkehrssteuerung erforderlich ist.**

   Fügen Sie den Modulnamen zur Spalte für das Metermodul in Ihrer QoS-Planungstabelle hinzu.

6. **Fügen Sie die Raten für jede zu messende Klasse in die Organisationstabelle ein.**

   Wenn Sie das Modul `tokenmt` verwenden, müssen Sie die folgenden Raten in Bit pro Sekunde definieren:

- Committed Rate
- Peak Rate

Wenn diese Raten ausreichen, um eine bestimmte Klasse zu messen, brauchen Sie nur die Committed Rate und in den Committed Burst für `tokenmt` definieren.

Falls erforderlich, können Sie auch die folgenden Raten definieren:

- Committed Burst
- Peak Burst

Eine vollständige Definition der `tokenmt`-Raten finden Sie unter „Konfiguration von `tokenmt` als Two-Rate Meter" auf Seite 911. Ausführliche Informationen finden Sie auch in der Manpage `tokenmt` (7ipp).

Wenn Sie das Modul `tswtclmt` verwenden, müssen Sie die folgenden Raten in Bit pro Sekunde definieren.

- Committed Rate
- Peak Rate

Sie können auch die Fenstergröße in Millisekunden definieren. Diese Raten sind unter „`tswtclmt`-Metermodul" auf Seite 912 und in der Manpage `twstclmt`(7ipp) definiert.

7. **Fügen Sie das Ergebnis der Datenverkehr-Konformität für den gemessenen Verkehr hinzu.**

   Das Ergebnis für beide Metermodule ist entweder grün, rot oder gelb. Fügen Sie Ihrer QoS-Organisationstabelle das Ergebnis für die Datenverkehr-Konformität hinzu, die für die von Ihnen definierten Raten gelten. Ergebnisse für die Metermodule sind unter „Metermodul" auf Seite 910 genauer beschrieben.

   Sie müssen festlegen, welche Aktionen für Verkehr durchgeführt werden soll, der der Committed Rate entspricht bzw. nicht entspricht. Häufig, aber nicht immer, ist diese Aktion das Markieren des Paket-Headers mit einem Per-Hop-Behavior. Eine akzeptable Aktion für Verkehr auf grüner Ebene ist das Fortsetzen der Verarbeitung, solange die Verkehrswerte die Committed Rate nicht überschreiten. Eine andere Aktion wäre das Abwerfen von Paketen einer Klasse, wenn Datenflüsse die Peak Rate überschreiten.

Beispiel 33–2 Definieren von Metermodulen

In der folgenden Tabelle, die als Beispiel dient, sind die Meter-Einträge für eine Klasse mit E-Mail-Verkehr aufgeführt. Das Netzwerk, in dem sich das IPQoS-Systemen befindet, verfügt über eine gesamte Bandbreite von 100 Mbit/s oder 10000000 Bit pro Sekunde. Die QoS-Richtlinie weist der E-Mail-Klasse eine niedrige Priorität zu. Darüber hinaus erhält diese Klasse das Weiterleitungsverhalten „Beste Leistung".

Klasse	Priorität	Filter	Selektor	Rate
email	8	mail_in	daddr10.50.50.5 dport imap direction LOCAL_IN	
email	8	mail_out	saddr10.50.50.5 sport imap direction LOCAL_OUT	meter=tokenmt Committed Rate=5000000 Committed Burst =5000000 Peak Rate =10000000 Peak Burst=1000000 Prioritätsstufe grün=Verarbeitung fortsetzen Prioritätsstufe gelb=mit gelbem PHB markieren Prioritätsstufe rot=Abwerfen

Siehe auch

- Informationen zum Definieren des Weiterleitungsverhaltens für Pakete, die zum Netzwerkstrom zurückkehren, finden Sie unter „So planen Sie das Weiterleitungsverhalten“ auf Seite 855.
- Informationen zum Planen des Flow Accounting für bestimmte Arten von Datenverkehr finden Sie unter „So planen Sie das Flow Accounting“ auf Seite 858.
- Informationen zum Hinzufügen weiterer Klassen zur QoS-Richtlinie finden Sie unter „So definieren Sie die Klassen für Ihre QoS-Richtlinie“ auf Seite 848.
- Informationen zum Hinzufügen weiterer Filter zur QoS-Richtlinie finden Sie unter „So definieren Sie Filter in der QoS-Richtlinie“ auf Seite 851.
- Informationen zum Definieren eines anderen Schemas zur Flusskontrolle finden Sie unter „So planen Sie die Verkehrssteuerung“ auf Seite 852.
- Informationen zum Erstellen einer IPQoS-Konfigurationsdatei finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.

▼ So planen Sie das Weiterleitungsverhalten

Das Weiterleitungsverhalten bestimmt die Priorität und Drop-Prioritätsstufe von Verkehrswerten, die in das Netzwerk weitergeleitet werden sollen. Grundsätzlich können Sie zwischen zwei Weiterleitungsverhalten wählen: Priorisieren der Datenströme einer Klasse in Relation zu anderen Verkehrsklassen oder vollständiges Abwerfen der Datenflüsse.

Das Diffserv-Modell verwendet den Marker, um Verkehrswerten das ausgewählte Weiterleitungsverhalten zuzuweisen. IPQoS bietet die folgenden Markermodule.

- `dscpmk` – Dient zum Markieren des DS-Feldes eines IP-Pakets mit einem DSCP
- `dlcosmk` – Dient zum Markieren des VLAN-Tags eines Datagramms mit einem Serviceklassen (Class of Service, CoS)-Wert

---

Hinweis – Die Vorschläge in diesem Abschnitt beziehen sich speziell auf IP-Pakete. Wenn Ihr IPQoS-System ein VLAN-Gerät umfasst, können Sie den Marker `dlcosmk` verwenden, um das Weiterleitungsverhalten für Datagramme festzulegen. Weitere Informationen hierzu finden Sie unter „Verwenden des Markers `dlcosmk` mit VLAN-Geräten“ auf Seite 915.

Um IP-Datenverkehr zu priorisieren, müssen Sie jedem Paket einen DSCP zuweisen. Der Marker `dscpmk` markiert das DS-Feld eines Pakets mit dem DSCP. Sie wählen den DSCP einer Klasse aus einer Gruppe bekannter Codepoints aus, die dem Weiterleitungsverhalten zugewiesen sind. Zu diesen bekannten Codepoints zählen 46 (101110) für das EF PHB und eine Reihe von Codepoints für den AF PHB. Eine Übersicht zu den DSCP und zur Weiterleitung finden Sie unter „Verkehrsweiterleitung in einem IPQoS-konformen Netzwerk“ auf Seite 836.

Bevor Sie beginnen Bei den nächsten Schritten wird davon ausgegangen, dass Sie Klassen und Filter für die QoS-Richtlinie definiert haben. Obwohl Sie den Meter mit dem Marker zur Steuerung von Datenverkehr verwenden werden, können Sie den Marker auch separat einsetzen, um ein Weiterleitungsverhalten zu definieren.

1. **Erstellen Sie eine Übersicht der bereits erstellten Klassen und die Prioritäten, die Sie jeder Klasse zugewiesen haben.**

   Nicht alle Verkehrsklassen müssen markiert werden.

2. **Weisen Sie der Klasse mit der höchsten Priorität das EF Per-Hop-Behavior zu.**

   Das EF PHB garantiert, dass Pakete mit dem EF DSCP 46 (101110) vor Paketen mit AF PHBs in das Netzwerk freigegeben werden. Verwenden Sie das EF PHB für Datenverkehr mit der höchste Priorität. Weitere Informationen zum EF finden Sie unter „Expedited Forwarding (EF) PHB“ auf Seite 914.

3. **Weisen Sie den Klassen, deren Datenverkehr gemessen werden muss, ein Weiterleitungsverhalten zu.**

4. **Weisen Sie den verbleibenden Klassen in Übereinstimmung mit den Prioritäten, die Sie diesen Klassen zugewiesen haben, DS Codepoints zu.**

Beispiel 33–3 QoS-Richtlinie für eine Spieleanwendung

Der Datenverkehr wird im Allgemeinen aus folgenden Gründen gemessen:

- Eine SLA garantiert Paketen dieser Klasse höheren Service oder geringerem Service, wenn das Netzwerk stark ausgelastet ist.
- Eine Klasse mit einer niedrigeren Priorität hat die Tendenz, das Netzwerk zu fluten.

Sie können den Marker mit dem Meter verwenden, um diesen Klassen Differentiated Services und Bandbreitenverwaltung bereitzustellen. Die folgende Tabelle zeigt beispielsweise einen Teil der QoS-Richtlinie. Diese Richtlinie definiert eine Klasse für eine beliebte Spieleanwendung, die einen starken Datenverkehr erzeugt.

Klasse	Priorität	Filter	Selektor	Rate	Weiterleitung?
games_app	9	games_in	sport 6080	entf.	entf.
games_app	9	games_out	dport 6081	meter=tokenmt Committed Rate=5000000 Committed Burst =5000000 Peak Rate =10000000 Peak Burst=15000000 Prioritätsstufe grün=Verarbeitung fortsetzen Prioritätsstufe gelb=mit gelbem PHB markieren Prioritätsstufe rot=Abwerfen	grün =AF31 gelb=AF42 rot=drop

Die Weiterleitungsverhalten weisen demgames_app-Datenverkehr, der seiner Committed Rate entspricht oder unter der Peak Rate liegt, DSCPs mit geringer Priorität zu. Wenn der games_app -Datenverkehr die Peak Rate übersteigt, gibt die QoS-Richtlinie an, dass Pakete von games_app abzuwerfen sind. Alle AF Codepoints sind in Tabelle 37–2 aufgeführt.

Siehe auch

- Informationen zum Planen des Flow Accounting für bestimmte Arten von Datenverkehr finden Sie unter „So planen Sie das Flow Accounting“ auf Seite 858.
- Informationen zum Hinzufügen weiterer Klassen zur QoS-Richtlinie finden Sie unter „So definieren Sie die Klassen für Ihre QoS-Richtlinie“ auf Seite 848.
- Informationen zum Hinzufügen weiterer Filter zur QoS-Richtlinie finden Sie unter „So definieren Sie Filter in der QoS-Richtlinie“ auf Seite 851.
- Informationen zum Definieren eines Schemas für die Flusskontrolle finden Sie unter „So planen Sie die Verkehrssteuerung“ auf Seite 852.

- Informationen zum Definieren zusätzlicher Weiterleitungsverhalten für Datenstöme, die zum Netzwerkstrom zurückkehren, finden Sie unter „So planen Sie das Weiterleitungsverhalten“ auf Seite 855.
- Informationen zum Erstellen einer IPQoS-Konfigurationsdatei finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.

▼ So planen Sie das Flow Accounting

Sie verwenden das IPQoS-Modul `flowacct`, um Verkehrswerte zur Fakturierung und Netzwerkverwaltung zu verfolgen. Gehen Sie nach dem folgenden Verfahren vor, um festzustellen, ob Ihre QoS-Richtlinie das Flow Accounting umfassen soll.

1. **Bietet Ihr Unternehmen seinen Kunden SLAs an?**

   In diesem Fall sollten Sie das Flow Accounting verwenden. Erstellen Sie eine Übersicht der SLAs, um festzustellen, welche Arten des Netzwerkverkehrs Ihr Unternehmen seinen Kunden in Rechnung stellen möchte. Dann prüfen Sie in Ihrer QoS-Richtlinie, welche Klassen zu berechnenden Verkehr auswählen.

2. **Gibt es Anwendungen, die überwacht oder überprüft werden müssen, um Netzwerkprobleme zu vermeiden?**

   In diesem Fall sollten Sie das Flow Accounting einsetzen, um das Verhalten dieser Anwendungen zu beobachten. Ermitteln Sie in Ihrer QoS-Richtlinie die Klassen, denen Sie Verkehr zugewiesen haben, der überwacht werden muss.

3. **Kennzeichnen Sie jede Klasse, für die das Flow Accounting erforderlich ist, in Ihrer QoS-Planungstabelle mit einem „J“ in der Flow Accounting-Spalte.**

Siehe auch

- Informationen zum Hinzufügen weiterer Klassen zur QoS-Richtlinie finden Sie unter „So definieren Sie die Klassen für Ihre QoS-Richtlinie“ auf Seite 848.
- Informationen zum Hinzufügen weiterer Filter zur QoS-Richtlinie finden Sie unter „So definieren Sie Filter in der QoS-Richtlinie“ auf Seite 851.
- Informationen zum Definieren eines Schemas für die Flusskontrolle finden Sie unter „So planen Sie die Verkehrssteuerung“ auf Seite 852.
- Informationen zum Definieren des Weiterleitungsverhaltens für Pakete, die zum Netzwerkstrom zurückkehren, finden Sie unter „So planen Sie das Weiterleitungsverhalten“ auf Seite 855.
- Informationen zum Planen von zusätzlichem Flow Accounting für bestimmte Arten von Datenverkehr finden Sie unter „So planen Sie das Flow Accounting“ auf Seite 858.

- Informationen zum Erstellen einer IPQoS-Konfigurationsdatei finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.

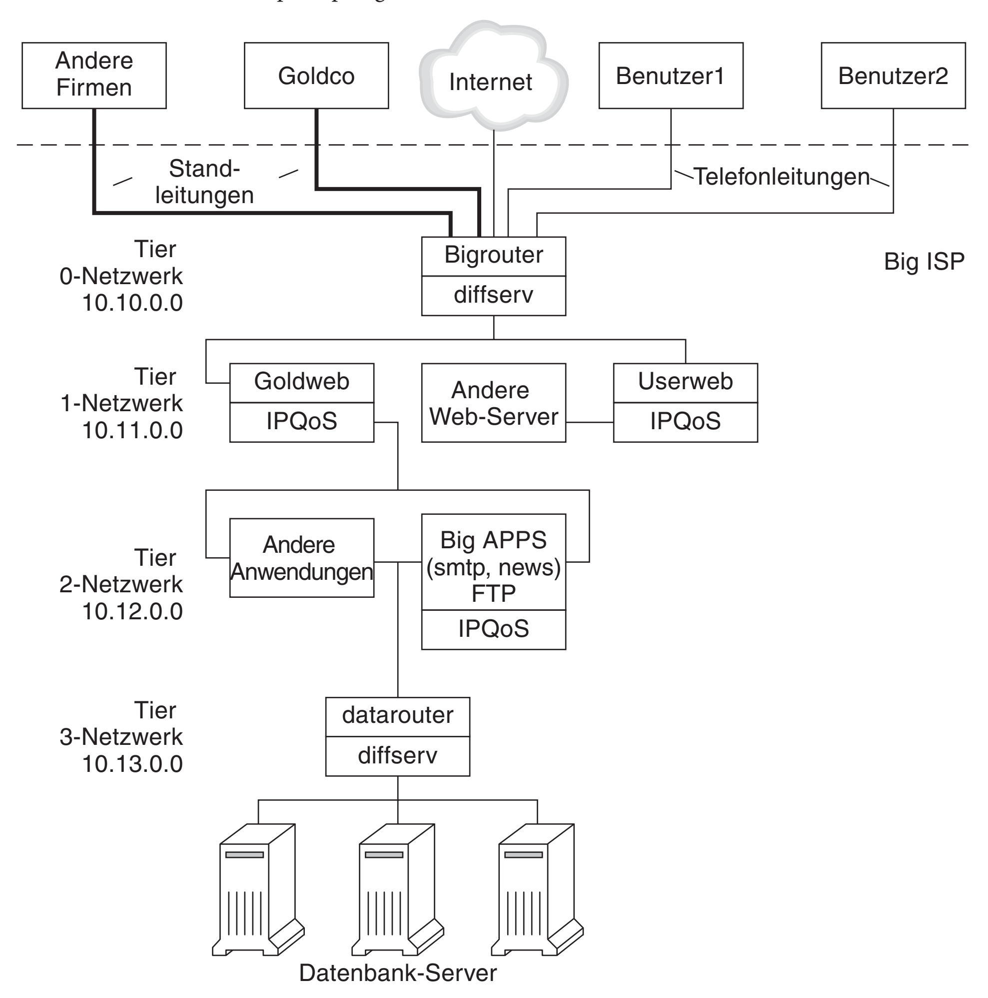
Einführung in das IPQoS-Konfigurationsbeispiel

Die Aufgaben in den verbleibenden Kapiteln dieses Handbuchs verwenden die in diesem Abschnitt vorgestellte IPQoS-Beispielkonfiguration. In diesem Beispiel wird gezeigt die Differentiated Services -Lösung im öffentlichen Intranet von BigISP, einem fiktiven Service Provider. BigISP bietet großen Unternehmen, die ihre Verbindungen zu BigISP über Standleitungen herstellen, Services an. Einzelpersonen, die sich über Modems einwählen, können ebenfalls Services von BigISP erwerben.

IPQoS-Topologie

Die folgende Abbildung zeigt die Netzwerktopologie des öffentlichen Intranet von BigISP.

ABBILDUNG 33–4 IPQoS-Beispieltopologie



BigISP hat die folgenden vier Tiers in seinen öffentlichen Intranet implementiert:

- **Tier 0** – Netzwerk `10.10.0.0` umfasst einen großen Diffserv-Router namens `Bigrouter`, der über externe und interne Schnittstellen verfügt. Mehrere Unternehmen, einschließlich einem großen Unternehmen namens Goldco, haben Standleitungsservices gemietet, die an `Bigrouter` enden. Tier 0 bedient darüber hinaus Einzelpersonen, die sich über Telefonleitungen oder ISDN einwählen.
- **Tier 1** – Netzwerk `10.11.0.0` stellt Webservices bereit. Der Server `Goldweb` fungiert als Host für die Website, die von Goldco als Teil des Premium-Services von BigISP erworben hat. Der Server `Userweb` fungiert als Host für kleine Websites, die von einzelnen Kunden erworben wurden. Sowohl `Goldweb` als auch `Userweb` sind IPQoS-konform.

- **Tier 2** – Netzwerk `10.12.0.0` stellt allen Kunden Anwendungen bereiten. `BigAPPS`, einer der Anwendungsserver, ist IPQoS-konform. `BigAPPS` bietet SMTP-, News- und FTP-Services.
- **Tier 3** – Netzwerk `10.13.0.0` beherbergt große Datenbankserver. Zugriff auf Tier 3 wird von `datarouter`, einem Diffserv-Router kontrolliert.

KAPITEL 34

Erstellen der IPQoS-Konfigurationsdatei (Aufgaben)

In diesem Kapitel wird gezeigt, wie Sie IPQoS-Konfigurationsdateien erstellen. Die folgenden Themen behandelt.

- „Definieren einer QoS-Richtlinie in der IPQoS-Konfigurationsdatei (Übersicht der Schritte)" auf Seite 863
- „Tools zum Erstellen einer QoS-Richtlinie" auf Seite 865
- „Erstellen von IPQoS-Konfigurationsdateien für Webserver" auf Seite 866
- „Erstellen einer IPQoS-Konfigurationsdateien für einen Anwendungsserver" auf Seite 880
- „Bereitstellen von Differentiated Services auf einem Router" auf Seite 890

In diesem Kapitel wird davon ausgegangen, dass Sie eine vollständige QoS-Richtlinie definiert haben und bereit sind, diese Richtlinie als Basis für die IPQoS-Konfigurationsdatei zu verwenden. Anweisungen zur Planung einer QoS-Richtlinie finden Sie unter „Planen der Quality of Service-Richtlinie" auf Seite 845.

Definieren einer QoS-Richtlinie in der IPQoS-Konfigurationsdatei (Übersicht der Schritte)

In der folgenden Tabelle sind die allgemeinen Aufgaben zum Erstellen einer IPQoS-Konfigurationsdatei aufgeführt, sowie die Links zu den Abschnitten, in denen die Schritte zum Durchführen dieser Aufgaben beschrieben sind.

Aufgabe	Beschreibung	Siehe
1. Planen Ihrer IPQoS konformen Netzwerkkonfiguration.	Entscheiden Sie, welche Systeme in lokalen Netzwerken IPQoS-konform werden sollen.	„So bereiten Sie ein Netzwerk für IPQoS vor" auf Seite 847

Aufgabe	Beschreibung	Siehe
2. Planen der QoS-Richtlinie für IPQoS-Systeme in Ihrem Netzwerk.	Kategorisieren Sie die Verkehrswerte in einzelne Serviceklassen. Dann legen Sie fest, für welchen Verkehr Verkehrsmanagement erforderlich ist.	„Planen der Quality of Service-Richtlinie" auf Seite 845
3. Erstellen der IPQoS-Konfigurationsdatei und Definieren der ersten Aktion.	Erstellen Sie die IPQoS-Datei, rufen Sie den IP-Classifier auf und definieren Sie eine Klasse für die Verarbeitung.	„So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen" auf Seite 868
4. Erstellen von Filtern für eine Klasse.	Fügen Sie die Filter hinzu, mit denen der Datenverkehr ausgewählt und in einer Klasse strukturiert wird.	„So definieren Sie Filter in der IPQoS-Konfigurationsdatei" auf Seite 870
5. Hinzufügen weiterer Klassen und Filter zur IPQoS-Konfigurationsdatei.	Erstellen Sie weitere Klassen und Filter, die vom IP-Classifier bearbeitet werden.	„So erstellen Sie eine IPQoS-Konfigurationsdatei für einen Beste Leistung-Webserver" auf Seite 877
6. Hinzufügen einer `action`-Anweisung mit Parametern, mit der die Metermodule konfiguriert werden.	Wenn die QoS-Richtlinie eine Verkehrssteuerung verlangt, weisen Sie dem Meter Verkehrssteuerungraten und Konformitätsebenen zu.	„So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei" auf Seite 887
7. Hinzufügen einer `action`-Anweisung mit Parametern, mit der der Marker konfiguriert wird.	Wenn die QoS-Richtlinie differenzierte Weiterleitungsverhalten verlangt, legen Sie fest, wie Datenverkehrsklassen weitergeleitet werden sollen.	„So definieren Sie das Weiterleiten von Datenverkehr in der IPQoS-Konfigurationsdatei" auf Seite 872
8. Hinzufügen einer `action`-Anweisung mit Parametern, mit der die das Flow Accounting-Modul konfiguriert wird.	Wenn die QoS-Richtlinie Statistiken zu den Verkehrswerten verlangt, legen Sie fest, wie die Accounting-Statistiken gesammelt werden.	„So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei" auf Seite 875
9. Übernehmen der IPQoS-Konfigurationsdatei.	Fügen Sie den Inhalt der angegebenen IPQoS-Konfigurationsdatei zu den entsprechenden Kernel-Modulen hinzu.	„So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module" auf Seite 894

Aufgabe	Beschreibung	Siehe
10. Konfigurieren des Weiterleitungsverhalten in den Router-Dateien.	Wenn eine IPQoS-Konfigurationsdatei im Netzwerk das Weiterleitungsverhalten definiert, fügen Sie die resultierenden DSCPs zu den entsprechenden Scheduling-Dateien auf dem Router hinzu.	„So konfigurieren Sie einen Router in einem IPQoS-konformen Netzwerk" auf Seite 890

Tools zum Erstellen einer QoS-Richtlinie

Die QoS-Richtlinie für Ihr Netzwerk befindet sich in der IPQoS-Konfigurationsdatei. Diese Konfigurationsdatei erstellen Sie mit einem Texteditor. Dann stellen Sie die Datei als ein Argument für `ipqosconf`, dem IPQoS-Konfigurationsprogramm, bereit. Wenn Sie `ipqosconf` anweisen, die in Ihrer Konfigurationsdatei definierte Richtlinie anzuwenden, wird die Richtlinie in das Kernel-IPQoS-System geschrieben. Ausführliche Informationen zum Befehl `ipqosconf` finden Sie in der Manpage `ipqosconf`(1M). Anweisungen zur Verwendung von `ipqosconf`, finden Sie unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module" auf Seite 894.

Allgemeine IPQoS-Konfigurationsdatei

Eine IPQoS-Konfigurationsdatei besteht aus mehreren `action`-Anweisungen, über die die QoS-Richtlinie umgesetzt wird, die Sie unter „Planen der Quality of Service-Richtlinie" auf Seite 845 definiert haben. Die IPQoS-Konfigurationsdatei konfiguriert die IPQoS-Module. Jede action-Anweisung enthält einen Satz mit *Klassen*, *Filtern* oder *Parametern*, die von dem Modul verarbeitet wird, das in der action-Anweisung aufgerufen wird.

Die vollständige Syntax der IPQoS-Konfigurationsdatei finden Sie in Beispiel 37–3 und in der Manpage `ipqosconf`(1M).

Konfigurieren der IPQoS-Beispieltopologie

Die Aufgaben in diesem Kapitel klären, wie die IPQoS-Konfigurationsdateien für drei IPQoS-konforme Systeme erstellt werden. Diese Systeme sind Teil der Netzwerktopologie des Unternehmens BigISP, das in Abbildung 33–4 vorgestellt wurde.

- `Goldweb` – Ein Webserver, der als Host für die Websites der Kunden dient, die Premium-Level SLAs erworben haben
- `Userweb` – Ein weniger leistungsstarker Webserver, der als Host für die Websites von privaten Kunden dient, die „Beste Leistung" SLAs erworben haben

- BigAPPS – Ein Anwendungsserver, der E-Mail-, Network News- und FTP-Services für Gold-Level und Beste Leistung-Kunden bereitstellt

Diese drei Konfigurationsdateien zeigen die am häufigsten verwendeten IPQoS-Konfigurationen. Sie können die Beispieldateien aus dem nächsten Abschnitt als Vorlagen für Ihre eigenen IPQoS-Implementierungen verwenden.

Erstellen von IPQoS-Konfigurationsdateien für Webserver

In diesem Abschnitt wird eine IPQoS-Konfigurationsdatei vorgestellt, mir deren Hilfe Ihnen gezeigt wird, wie eine Konfiguration für einen Premium-Webserver erstellt wird. Dann wird gezeigt, wie eine vollständig andere Serviceebene in einer Konfigurationsdatei für einen Server erstellt wird, der als Host für persönliche Websites dient. Beide Server sind Teil des Netzwerkbeispiels, das in Abbildung 33–4 vorgestellt wurde.

Die folgende Konfigurationsdatei definiert IPQoS-Aktivitäten für den Server Goldweb. Dieser Server dient als Host für die Website von Goldco, einem Unternehmen, das eine Premium-SLA erworben hat.

BEISPIEL 34–1 IPQoS-Beispielkonfigurationsdatei für einen Premium-Webserver

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name goldweb
        next_action markAF11
        enable_stats FALSE
    }
    class {
        name video
        next_action markEF
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class goldweb
    }
    filter {
        name videoout
        sport videosrv
        direction LOCAL_OUT
        class video
    }
}
```

BEISPIEL 34–1 IPQoS-Beispielkonfigurationsdatei für einen Premium-Webserver *(Fortsetzung)*

```
action {
    module dscpmk
    name markAF11
    params {
        global_stats FALSE
        dscp_map{0-63:10}
        next_action continue
    }
}
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
action {
    module flowacct
    name acct
    params {
        enable_stats TRUE
        timer 10000
        timeout 10000
        max_limit 2048
    }
}
```

Die folgende Konfigurationsdatei definiert IPQoS-Aktivitäten für den Server `Userweb`. Dieser Server dient als Host für Privatkunden mit kostengünstigen oder *Beste Leistung*-SLAs. Diese Serviceebene garantiert den besten Service, der einem Beste Leistung-Kunden bereitgestellt werden kann, nachdem das IPQoS-System den Datenverkehr von Kunden mit teureren SLAs verarbeitet hat.

BEISPIEL 34–2 IPQoS-Beispielkonfigurationsdatei für einen Beste Leistung-Webserver

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name Userweb
        next_action markAF12
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
```

BEISPIEL 34–2 IPQoS-Beispielkonfigurationsdatei für einen Beste Leistung-Webserver *(Fortsetzung)*

```
        direction LOCAL_OUT
        class Userweb
   }
}
action {
    module dscpmk
    name markAF12
    params {
        global_stats FALSE
        dscp_map{0-63:12}
        next_action continue
    }
}
```

▼ So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen

Sie können Ihre erste IPQoS-Konfigurationsdatei in einem beliebigen Verzeichnis erstellen. Wählen Sie das Verzeichnis, das Sie am einfachsten verwalten können. Die Aufgaben in diesem Kapitel verwenden das `/var/ipqos` als Speicherort für die IPQoS-Konfigurationsdateien. Im folgenden Verfahren wird das interne Segment der IPQoS-Konfigurationsdatei erstellt, die in Beispiel 34–1 eingeführt wurde.

Hinweis – Achten Sie beim Erstellen der IPQoS-Konfigurationsdatei darauf, die `action`-Anweisung und -Klausel mit geschweiften Klammern zu beginnen und zu beenden ({ }). Ein Beispiel für die Verwendung der Klammern finden Sie in Beispiel 34–1.

---

1. **Melden Sie sich beim Premium-Webserver an und erstellen Sie eine neue IPQoS-Konfigurationsdatei mit der Erweitung `.qos`.**

   Jede IPQoS-Konfigurationsdatei muss mit der Versionsnummer `fmt_version 1.0` als erste unkommentierte Zeile beginnen.

2. **Nach dem Eröffnungsparameter muss die erste `action`-Anweisung folgen, die den generischen IP-Classifier `ipgpc` konfiguriert.**

   Diese erste Aktion beginnt die Baumstruktur der `action`-Anweisungen, aus denen sich die IPQoS-Konfigurationsdatei zusammensetzt. Die Datei `/var/ipqos/Goldweb.qos` beginnt z. B. mit der ersten `action`-Anweisung, die den `ipgpc`-Classifier aufruft.

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
```

`fmt_version 1.0`	Beginnt die IPQoS-Konfigurationsdatei.

`action {`	Beginnt die action-Anweisung.
`module ipgpc`	Konfiguriert den `ipgpc`-Classifier als die erste Aktion in der Konfigurationsdatei.
`name ipgpc.classify`	Definiert den Namen der `action`-Anweisung des Classifiers, der stets `ipgpc.classify` lauten muss.

Ausführliche syntaktische Informationen zu den `action`-Anweisungen finden Sie unter „`action`-Anweisung“ auf Seite 921 und in der Manpage `ipqosconf`(1M).

3 Fügen Sie eine `params`-Klausel mit dem Statistik-Parameter `global_stats` hinzu.

```
params {
          global_stats TRUE
   }
```

Mit dem Parameter `global_stats TRUE` in der `ipgpc.classify`-Anweisung können Sie das Erfassen von Statistiken für diese Aktion aktivieren. `global_stats TRUE` aktiviert darüber hinaus das Erfassen von Statistiken pro Klasse, wenn eine Klassenklauseldefinition `enable_stats TRUE` angibt.

Das Aktivieren der Statistiken verbessert die Leistung. Vielleicht möchten Sie Statistiken zu der neuen IPQoS-Konfigurationsdatei erfassen, um zu prüfen, ob die IPQoS ordnungsgemäß arbeitet. Später können Sie das Erfassen von Statistiken deaktivieren, indem Sie das Argument von `global_stats` zu `FALSE` ändern.

Globale Statistiken sind nur ein Parametertyp, den Sie in einer `params`-Klausel definieren können. Sytaktische and sonstige Details zu den `params`-Klauseln finden Sie unter „`params`-Klausel“ auf Seite 924 und in der Manpage `ipqosconf(1M)`.

4 Definieren Sie eine Klasse, die den Datenverkehr identifiziert, der für den Premium-Server bestimmt ist.

```
class {
        name goldweb
        next_action markAF11
        enable_stats FALSE
    }
```

Diese Anweisung wird als *class-Klausel* bezeichnet. Eine `class`-Klausel hat den folgenden Inhalt.

name goldweb	Erstellt die Klasse `goldweb`, um den Datenverkehr zu identifizieren, der für den Server `Goldweb` bestimmt ist.
next_action markAF11	Weist das `ipgpc`-Modul an, Pakete der `goldweb`-Klasse an die action-Anweisung `markAF11` zu übergeben. Die action-Anweisung `markAF11` ruft den Marker `dscpmk` auf.
enable_stats FALSE	Aktiviert die Erfassung von Statistiken für die Klasse `goldweb.` Da der Wert für `enable_stats FALSE` lautet, werden keine Statistiken

für diese Klasse erfasst.

Ausführliche Informationen zur Syntax der `class`-Klausel finden Sie unter „`class`-Klausel“ auf Seite 923 und in der Manpage `ipqosconf`(1M).

5 **Definieren Sie eine Klasse, die eine Anwendung kennzeichnet, die Weiterleitungen mit der höchsten Priorität aufweist.**

```
class {
        name video
        next_action markEF
        enable_stats FALSE
    }
```

`name video`	Erstellt die Klasse `video`, um Streaming Video-Datenverkehr zu identifizieren, der vom Server `Goldweb` ausgeht.
`next_action markEF`	Weist das `ipgpc`-Modul an, Pakete der `video`-Klasse an die `markEF`-Anweisung zu übergeben, nachdem `ipgpc` die Bearbeitung vollständig abgeschlossen hat. Die Anweisung `markEF` ruft den Marker `dscpmk` auf.
`enable_stats FALSE`	Aktiviert die Erfassung von Statistiken für die Klasse `video.` Da der Wert für `enable_stats FALSE` lautet, werden keine Statistiken für diese Klasse erfasst.

Siehe auch

- Informationen zum Definieren von Filtern für die gerade erstellte Klasse finden Sie unter „So definieren Sie Filter in der IPQoS-Konfigurationsdatei“ auf Seite 870.
- Informationen zum Erstellen einer weiteren class-Klausel für die Konfigurationsdatei finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.

▼ So definieren Sie Filter in der IPQoS-Konfigurationsdatei

Im nächsten Verfahren wird gezeigt, wie Sie Filter in der IPQoS-Konfigurationsdatei definieren.

Bevor Sie beginnen

Bei diesem Verfahren wird davon ausgegangen, dass Sie die Datei bereits erstellt und mit der Definition der Klassen begonnen haben. Mit den folgenden Schritten wird die Datei `/var/ipqos/Goldweb.qos` erweitert, die Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868 erstellt haben.

Hinweis – Achten Sie beim Erstellen der IPQoS-Konfigurationsdatei darauf, jede `class`- und `filter`-Klausel mit geschweiften Klammen zu beginnen und zu beenden ({ }). Ein Beispiel für die Verwendung der Klammern finden Sie in Beispiel 34–1.

---

1. **Öffnen Sie die IPQoS-Konfigurationsdatei und suchen Sie das Ende der letzten von Ihnen definierten Klasse.**

   Bei dem IPQoS-konformen Server `Goldweb` beginnen Sie z. B. hinter der `class`-Klausel, die Sie in `/var/ipqos/Goldweb.qos` erstellt haben:

```
class {
        name video
        next_action markEF
        enable_stats FALSE
    }
```

2. **Definieren Sie eine `filter`-Klausel, um den abgehenden Datenverkehr vom IPQoS-System auszuwählen.**

```
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class goldweb
    }
```

`name webout`	Benennt den Filter mit `webout`.
`sport 80`	Wählt Datenverkehr mit dem Ursprungs-Port 80 aus, dem bekannten Port für HTTP (Web)-Verkehr.
`direction LOCAL_OUT`	Wählt außerdem Verkehr aus, der vom lokalen System abgeht.
`class goldweb`	Identifiziert die Klasse, zu der der Filter gehört, in diesem Fall die Klasse `goldweb`.

   Syntaktische und ausführliche Informationen zur `filter`-Klausel in der IPQoS-Konfigurationsdatei finden Sie unter „`filter`-Klausel“ auf Seite 923.

3. **Definieren Sie eine `filter`-Klausel, um den Streaming Video-Datenverkehr vom IPQoS-System auszuwählen.**

```
    filter {
        name videoout
        sport videosrv
        direction LOCAL_OUT
        class video
    }
```

name videoout	Benennt den Filter mit `videoout`.

`sport videosrv`	Wählt Datenverkehr mit einem Ursprungs-Port von `videosrv` aus, ein zuvor definierter Port für die Streaming Video-Anwendung auf diesem System.
`direction LOCAL_OUT`	Wählt außerdem Verkehr aus, der vom lokalen System abgeht.
`class video`	Identifiziert die Klasse, zu der der Filter gehört, in diesem Fall die Klasse `video`.

Siehe auch

- Informationen zum Definieren des Weiterleitungsverhalten für die Markermodule finden Sie unter „So definieren Sie das Weiterleiten von Datenverkehr in der IPQoS-Konfigurationsdatei“ auf Seite 872.
- Informationen zum Definieren der Flusskontrolle-Parameter für die Metermodule finden Sie unter „So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei“ auf Seite 887.
- Informationen zum Aktivieren der IPQoS-Konfigurationsdatei finden Sie unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module“ auf Seite 894.
- Informationen zum Definieren von zusätzlichen Filtern finden Sie unter „So definieren Sie Filter in der IPQoS-Konfigurationsdatei“ auf Seite 870.
- Informationen zum Erstellen von Klassen für Verkehrswerte von Anwendungen finden Sie unter „So konfigurieren Sie die IPQoS-Konfigurationsdatei für einen Anwendungsserver“ auf Seite 882.

▼ So definieren Sie das Weiterleiten von Datenverkehr in der IPQoS-Konfigurationsdatei

Im nächsten Verfahren wird gezeigt, wie Sie das Weiterleiten von Datenverkehr definieren, indem Sie Per-Hop-Behaviors für eine Klasse in die IPQoS-Konfigurationsdatei einfügen.

Bevor Sie beginnen

Bei diesem Verfahren wird davon ausgegangen, dass Sie bereits eine IPQoS-Konfigurationsdatei erstellt und Klassen und Filter definiert haben. Mit den folgenden Schritten wird die Datei `/var/ipqos/Goldweb.qos` aus Beispiel 34–1 erweitert.

Hinweis – In diesem Verfahren wird gezeigt, wie Sie Weiterleitung von Datenverkehr mithilfe des Markermoduls `dscpmk` konfigurieren. Informationen zum Weiterleiten von Datenverkehr in VLAN-Systemen mithilfe des Markers `dlclosmk` finden Sie unter „Verwenden des Markers `dlcosmk` mit VLAN-Geräten“ auf Seite 915.

---

1 Öffnen Sie die IPQoS-Konfigurationsdatei und suchen Sie das Ende des letzten von Ihnen definierten Filters.

Bei dem IPQoS-konformen Server `Goldweb` beginnen Sie z. B. hinter der `filter`-Klausel, die Sie in `/var/ipqos/Goldweb.qos` erstellt haben:

```
filter {
        name videoout
        sport videosrv
        direction LOCAL_OUT
        class video
    }
}
```

Beachten Sie, dass sich diese `filter`-Klausel am Ende `action`-Anweisung des `ipgpc`-Classifiers befindet. Aus diesem Grund benötigen Sie eine schließende geschweifte Klammer, um den Filter zu beenden und eine zweite schließende geschweifte Klammer, um die `action`-Anweisung zu beenden.

2 Rufen Sie den Marker mit der folgenden `action`-Anweisung auf.

```
action {
    module dscpmk
    name markAF11
```

module dscpmk — Ruft das Markermodul `dscpmk` auf.

name markAF11 — Benennt die `action` -Anweisung mit `markAF11`.

Die zuvor definierte Klasse `goldweb` umfasst eine `next_action` `markAF11`-Anweisung. Diese Anweisung sendet Verkehrswerte an die action-Anweisung `markAF11`, nachdem der Classifier die Verarbeitung beendet hat.

3 Definieren Sie Aktionen, die der Marker am Verkehrswert durchführen soll.

```
    params {
        global_stats FALSE
        dscp_map{0-63:10}
        next_action continue
    }
}
```

global_stats FALSE — Aktiviert die Erfassung von Statistiken für die Marker `action`-Anweisung `markAF11.` Da der Wert für `enable_stats FALSE` lautet, werden keine Statistiken erfasst.

dscp_map{0–63:10} — Weist den Paket-Headern der Datenverkehrklasse `goldweb`, die momentan vom Marker verarbeitet werden, einen DSCP von `10` zu.

next_action continue — Gibt an, dass keine weitere Verarbeitung für die Pakete der Datenverkehrsklasse `goldweb` erforderlich sind, und dass diese Pakete in den Netzwerkdatenfluss zurückkehren können.

Der DSCP `10` weist den Marker an, alle Einträge in der `dscp`-Map auf den Dezimalwert 10 (binär 001010) zu setzen. Dieser Codepoint kennzeichnet, dass Pakete der Verkehrsklasse `goldweb` dem Per-Hop-Behavior AF11 unterliegen. AF11 stellt sicher, dass alle Pakete mit dem DSCP `10` einen low-drop-Service mit hoher Priorität erhalten. Somit erhält abgehender Datenverkehr für Premium-Kunden auf `Goldweb` die höchste Priorität, die für das Assured Forwarding (AF) PHB verfügbar ist. Eine Liste der möglichen DSCPs für AF finden Sie in Tabelle 37–2.

4 **Starten Sie eine weitere Marker `action`-Anweisung.**

```
action {
    module dscpmk
    name markEF
```

module dscpmk — Ruft das Markermodul `dscpmk` auf.

`name markEF` — Benennt die `action`-Anweisung mit `markEF`.

5 **Definieren Sie Aktionen, die der Marker am Verkehrswert durchführen soll.**

```
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

`global_stats TRUE` — Aktiviert die Erfassung von Statistiken für die `video`-Klasse, die Streaming Video-Pakete auswählt.

`dscp_map{0–63:46}` — Weist den Paket-Headern der Datenverkehrklasse `video`, die momentan vom Marker verarbeitet werden, einen DSCP von `46` zu.

`next_action acct` — Weist das `dscpmk`-Modul an, Pakete der `video`-Klasse an die `action`-Anweisung `acct` weiterzuleiten, nachdem `dscpmk` die Bearbeitung vollständig abgeschlossen hat. Die `action`-Anweisung `acct` ruft das `flowacct`-Modul auf.

Der DSCP `46` weist das `dscpmk`-Modul an, alle Einträge in der `dscp`-Map im DS-Feld auf den Dezimalwert 46 (binär 101110) zu setzen. Dieser Codepoint kennzeichnet, dass Pakete der Verkehrsklasse `video` dem Per-Hop-Behavior Expedited Forwarding (EF) unterliegen.

Hinweis – Der empfohlene Codepoint für EF ist 46 (binär 101110). Andere DSCPs weisen einem Paket AF PHBs zu.

Das EF PHB garantiert, dass Pakete mit einem DSCP von `46` von IPQoS- und Diffserv-konformen Systemen die höchste Prioritätsstufe erhalten. Streaming-Anwendungen erfordern einen Service mit höchster Priorität. Dies ist der Grund, warum

Streaming-Anwendungen die EF PHBs in der QoS-Richtlinie zugeordnet sind. Weitere Einzelheiten zum Expedited Forwarding PHB finden Sie unter „Expedited Forwarding (EF) PHB“ auf Seite 914.

6 **Fügen Sie die gerade erstellten DSCPs zu den entsprechenden Dateien auf dem Diffserv-Router hinzu.**

Weitere Informationen hierzu finden Sie unter „So konfigurieren Sie einen Router in einem IPQoS-konformen Netzwerk“ auf Seite 890.

Siehe auch

- Informationen zum Erfassen von Flow Accounting-Statistiken bei Verkehrswerten finden Sie unter „So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei“ auf Seite 875.
- Informationen zum Definieren des Weiterleitungsverhalten für die Markermodule finden Sie unter „So definieren Sie das Weiterleiten von Datenverkehr in der IPQoS-Konfigurationsdatei“ auf Seite 872.
- Informationen zum Definieren der Flusskontrolle-Parameter für die Metermodule finden Sie unter „So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei“ auf Seite 887.
- Informationen zum Aktivieren der IPQoS-Konfigurationsdatei finden Sie unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module“ auf Seite 894.
- Informationen zum Definieren von zusätzlichen Filtern finden Sie unter „So definieren Sie Filter in der IPQoS-Konfigurationsdatei“ auf Seite 870.
- Informationen zum Erstellen von Klassen für Verkehrswerte von Anwendungen finden Sie unter „So konfigurieren Sie die IPQoS-Konfigurationsdatei für einen Anwendungsserver“ auf Seite 882.

▼ So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei

Hier wird gezeigt, wie Sie das Accounting für eine Datenverkehrsklasse in der IPQoS-Konfigurationsdatei aktivieren. In dem Verfahren wird gezeigt, wie Sie das Flow Accounting für die `video`-Klasse definieren, die unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868 eingeführt wurde. Diese Klasse wählt Streaming Video-Datenverkehr aus, der im Rahmen einer Premium-SLA eines Kunden berechnet werden muss.

Bevor Sie beginnen

Bei diesem Verfahren wird davon ausgegangen, dass Sie bereits eine IPQoS-Konfigurationsdatei erstellt und Klassen, Filter, Meteraktionen (sofern anwendbar) und

Markerungsoptionen (sofern anwendbar) erstellt haben. Mit den folgenden Schritten wird die Datei `/var/ipqos/Goldweb.qos` aus Beispiel 34–1 erweitert.

1. **Öffnen Sie die IPQoS-Konfigurationsdatei und suchen Sie das Ende der letzten von Ihnen definierten `action`-Anweisung.**

   Bei dem IPQoS-konformen Server `Goldweb` beginnen Sie z. B. hinter der `action`-Anweisung `markEF` in der Datei `/var/ipqos/Goldweb.qos`.

```
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

2. **Beginnen Sie eine `action`-Anweisung, mit der das Flow Accounting aufgerufen wird.**

```
action {
    module flowacct
    name acct
```

`module flowacct`	Ruft das Flow Accounting-Modul `flowacct` auf.
`name acct`	Benennt die `action`-Anweisung mit `acct`

3. **Definieren Sie eine `params`-Klausel, um das Accounting in der Datenverkehrsklasse zu steuern.**

```
params {
        global_stats TRUE
        timer 10000
        timeout 10000
        max_limit 2048
        next_action continue
    }
}
```

`global_stats TRUE`	Aktiviert die Erfassung von Statistiken für die `video`-Klasse, die Streaming Video-Pakete auswählt.
`timer 10000`	Gibt die Dauer des Intervalls in Millisekunden an, in dem die Flow-Tabelle nach abgelaufenen Flows gescannt wird. Bei diesem Parameter lautet das Intervall 10.000 ms.
`timeout 10000`	Gibt das Mindestintervall für den Timeout-Wert an. Ein Flow „läuft ab“ (times out), wenn die Pakete für den Flow nicht innerhalb eines Timeout-Intervalls erfasst werden. Bei diesem Parameter laufen die Pakete nach 10.000 ms ab.
`max_limit 2048`	Richtet die Höchstzahl der aktiven Flow-Datensätze in der Flow-Tabelle für diese Aktionsinstanz ein.

`next_action continue`	Gibt an, dass keine weitere Verarbeitung für die Pakete der Datenverkehrsklasse `video` erforderlich sind, und dass diese Pakete in den Netzwerkdatenfluss zurückkehren können.

Das `flowacct`-Modul erfasst Statistiken zu den Paket-Flows einer bestimmten Klasse, bis ein festgelegter `timeout`-Wert erreicht ist.

Siehe auch

- Informationen zur Konfiguration der Per-Hop-Behaviors auf einem Router finden Sie unter „So konfigurieren Sie einen Router in einem IPQoS-konformen Netzwerk“ auf Seite 890.
- Informationen zum Aktivieren der IPQoS-Konfigurationsdatei finden Sie unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module“ auf Seite 894.
- Informationen zum Erstellen von Klassen für Verkehrswerte von Anwendungen finden Sie unter „So konfigurieren Sie die IPQoS-Konfigurationsdatei für einen Anwendungsserver“ auf Seite 882.

▼ So erstellen Sie eine IPQoS-Konfigurationsdatei für einen Beste Leistung-Webserver

Die IPQoS-Konfigurationsdatei für einen Beste Leistung-Webserver unterscheidet sich nur wenig von einer IPQoS-Konfigurationsdatei für einen Premium-Webserver. Als Beispiel wird im folgenden Verfahren die Konfigurationsdatei aus Beispiel 34–2 verwendet.

1. **Melden Sie sich beim Beste Leistung-Webserver an.**

2. **Erstellen Sie eine neue IPQoS-Konfigurationsdatei mit der Erweiterung** `qos`**.**

```
fmt_vesion 1.0
action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
   }
```

Die Datei `/var/ipqos/userweb.qos` muss mit dem Teil einer `action`-Anweisung beginnen, die den `ipgpc`-Classifier aufruft. Darüber hinaus umfasst die `action`-Anweisung eine params-Klausel, um die Erfassung von Statistiken zu aktivieren. Eine Beschreibung dieser `action`-Anweisung finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.

3. **Definieren Sie eine Klasse, die den Datenverkehr identifiziert, der für den Beste Leistung-Server bestimmt ist.**

```
class {
        name userweb
```

```
        next_action markAF12
        enable_stats FALSE
    }
```

`name userweb`	Erstellt eine Klasse mit der Bezeichnung `userweb` zum Weiterleiten von Webverkehr von Benutzern.
`next_action markAF12`	Weist das `ipgpc`-Modul an, Pakete der `userweb`-Klasse an die `action`-Anweisung `markAF12` zu übergeben, nachdem `ipgpc` die Bearbeitung vollständig abgeschlossen hat. Die `action`-Anweisung `markAF12` ruft den `dscpmk`-Marker auf.
`enable_stats FALSE`	Aktiviert die Erfassung von Statistiken für die `userweb`-Klasse. Da der Wert für `enable_stats FALSE` lautet, werden keine Statistiken für diese Klasse erfasst.

Eine Beschreibung der `class`-Klausel finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen" auf Seite 868.

4 **Definieren Sie eine `filter`-Klausel, um den Verkehrswert für die `userweb`-Klasse auszuwählen.**

```
   filter {
       name webout
       sport 80
       direction LOCAL_OUT
       class userweb
   }
}
```

`name webout`	Benennt den Filter mit `webout`.
`sport 80`	Wählt Datenverkehr mit dem Ursprungs-Port 80 aus, dem bekannten Port für HTTP (Web)-Verkehr.
`direction LOCAL_OUT`	Wählt außerdem Verkehr aus, der vom lokalen System abgeht.
class userweb	Identifiziert die Klasse, zu der der Filter gehört, in diesem Fall die Klasse `userweb`.

Eine Beschreibung der `filter`-Klausel finden Sie unter „So definieren Sie Filter in der IPQoS-Konfigurationsdatei" auf Seite 870.

5 **Beginnen Sie die `action`-Anweisung, um den `dscpmk`-Marker aufzurufen.**

```
action {
    module dscpmk
    name markAF12
```

`module dscpmk`	Ruft das Markermodul `dscpmk` auf.
`name markAF12`	Benennt die `action` -Anweisung mit `markAF12`.

Die zuvor definierte Klasse `userweb` umfasst eine `next_action` `markAF12`-Anweisung. Diese Anweisung sendet Verkehrswerte an die `action`-Anweisung `markAF12`, nachdem der Classifier die Verarbeitung beendet hat.

6 **Definieren Sie die Parameter für den Marker, die bei der Verarbeitung des Verkehrswerts verwendet werden.**

```
    params {
        global_stats FALSE
        dscp_map{0-63:12}
        next_action continue
    }
}
```

`global_stats FALSE` — Aktiviert die Erfassung von Statistiken für die `markAF12` Marker `action`-Anweisung. Da der Wert für `enable_stats` `FALSE` lautet, werden keine Statistiken erfasst.

`dscp_map{0–63:12}` — Weist den Paket-Headern der Datenverkehrklasse `userweb`, die momentan vom Marker verarbeitet werden, einen DSCP von `12` zu.

next_action continue — Gibt an, dass keine weitere Verarbeitung für die Pakete der Datenverkehrsklasse `userweb` erforderlich sind, und dass diese Pakete in den Netzwerkdatenfluss zurückkehren können.

Der DSCP `12` weist den Marker an, alle Einträge in der `dscp`-Map auf den Dezimalwert 12 (binär 001100) zu setzen. Dieser Codepoint kennzeichnet, dass Pakete der Verkehrsklasse `userweb` dem Per-Hop-Behavior AF12 unterliegen. AF12 stellt sicher, dass alle Pakete mit dem DSCP `12` einen medium-drop-Service mit hoher Priorität erhalten.

7 **Nachdem Sie die IPQoS-Konfigurationsdatei vollständig erstellt haben, übernehmen Sie die Konfiguration.**

Siehe auch

- Informationen zum Hinzufügen von Klassen und der Konfiguration von Verkehrswerten anderer Anwendungen finden Sie unter „So konfigurieren Sie die IPQoS-Konfigurationsdatei für einen Anwendungsserver“ auf Seite 882.
- Informationen zur Konfiguration der Per-Hop-Behaviors auf einem Router finden Sie unter „So konfigurieren Sie einen Router in einem IPQoS-konformen Netzwerk“ auf Seite 890.
- Informationen zum Aktivieren der IPQoS-Konfigurationsdateien finden Sie unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module“ auf Seite 894.

Erstellen einer IPQoS-Konfigurationsdateien für einen Anwendungsserver

In diesem Abschnitt wird erklärt, wie Sie eine Konfigurationsdatei für einen Anwendungsserver erstellen, der Kunden wichtige Anwendungen bereitstellt. In diesem Verfahren wird der Server `BigAPPS` verwendet, der in Abbildung 33–4 vorgestellt wurde.

In der folgenden Konfigurationsdatei werden die IPQoS-Aktivitäten für den Server `BigAPPS` definiert. Dieser Server dient als Host für FTP, E-Mail (SMTP) und Network News (NNTP) für Kunden.

BEISPIEL 34–3 Beispiel einer IPQoS-Konfigurationsdatei für einen Anwendungsserver

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        next_action meterftp
    }
    filter {
        name smtpout
        sport smtp
        class smtp
    }
    filter {
        name newsout
        sport nntp
        class news
    }
    filter {
        name ftpout
        sport ftp
        class ftp
    }
   filter {
        name ftpdata
        sport ftp-data
        class ftp
    }
```

BEISPIEL 34–3 Beispiel einer IPQoS-Konfigurationsdatei für einen Anwendungsserver *(Fortsetzung)*

```
}
action {
    module dscpmk
    name markAF13
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
action {
    module tokenmt
    name meterftp
    params {
        committed_rate 50000000
        committed_burst 50000000
        red_action_name AF31
        green_action_name markAF22
        global_stats TRUE
    }
}
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

▼ So konfigurieren Sie die IPQoS-Konfigurationsdatei für einen Anwendungsserver

1 Melden Sie sich beim IPQoS-konformen Anwendungsserver an und erstellen Sie eine neue IPQoS-Konfigurationsdatei mit der Erweitung `.qos`.

Beispielsweise können Sie die Datei `/var/ipqos/BigAPPS.qos` für den Anwendungsserver erstellen. Beginnen Sie mit den folgenden erforderlichen Phrasen, um die `action`-Anweisung zu starten, die den `ipgpc`-Classifier aufruft:

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
```

Eine Beschreibung der einleitenden `action`-Anweisung finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen" auf Seite 868.

2 Erstellen Sie Klassen, um den Verkehr von drei Anwendungen auf BigAPPS-Server auszuwählen.

Fügen Sie die Klassendefinitionen hinter der einleitenden `action`-Anweisung ein.

```
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        enable_stats TRUE
        next_action meterftp
    }
```

`name smtp` — Erstellt eine Klasse namens `smtp`, die den E-Mail-Verkehrwert enthält, der von der SMTP-Anwendung verarbeitet wird.

`enable_stats FALSE` — Aktiviert die Erfassung von Statistiken für die `smtp`-Klasse. Da der Wert für `enable_stats FALSE` lautet, werden keine Statistiken für diese Klasse erfasst.

`next_action markAF13` — Weist das `ipgpc`-Modul an, Pakete der `smtp`-Klasse an die `action`-Anweisung `markAF13` zu übergeben, nachdem `ipgpc` die Bearbeitung vollständig abgeschlossen hat.

`name news`	Erstellt eine Klasse namens `news`, die den Network News-Verkehrswert enthält, der von der NNTP-Anwendung verarbeitet wird.
`next_action markAF21`	Weist das `ipgpc`-Modul an, Pakete der `news`-Klasse an die action-Anweisung `markAF21` zu übergeben, nachdem `ipgpc` die Bearbeitung vollständig abgeschlossen hat.
`name ftp`	Erstellt eine Klasse namens `ftp`, die den abgehenden Verkehr enthält, der von der FTP-Anwendung verarbeitet wird.
`enable_stats TRUE`	Aktiviert die Erfassung der Statistiken für die `ftp`-Klasse.
`next_action meterftp`	Weist das `ipgpc`-Modul an, Pakete der `ftp`-Klasse an die `action`-Anweisung `meterftp` zu übergeben, nachdem `ipgpc` die Bearbeitung vollständig abgeschlossen hat.

Weitere Informationen zum Definieren von Klassen finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.

3 **Definieren Sie `filter`-Klauseln, um den Datenverkehr der in Schritt 2 definierten Klassen auszuwählen.**

```
    filter {
        name smtpout
        sport smtp
        class smtp
    }
    filter {
        name newsout
        sport nntp
        class news
    }
        filter {
        name ftpout
        sport ftp
        class ftp
    }
        filter {
        name ftpdata
        sport ftp-data
        class ftp
    }
}
```

`name smtpout`	Benennt den Filter mit `smtpout`.
`sport smtp`	Wählt Datenverkehr mit dem Ursprungs-Port 25 aus, dem bekannten Port für die `sendmail` (SMTP)-Anwendung.
`class smtp`	Identifiziert die Klasse, zu der der Filter gehört, in diesem Fall die Klasse `smtp`.
`name newsout`	Benennt den Filter mit `newsout`.

`sport nntp`	Wählt Datenverkehr mit dem Ursprungs-Portnamen `nntp` aus, dem bekannten Portnamen für die Network News (NNTP)-Anwendung.
`class news`	Identifiziert die Klasse, zu der der Filter gehört, in diesem Fall die Klasse `news`.
`name ftpout`	Benennt den Filter mit `ftpout`.
`sport ftp`	Wählt Steuerungsdaten mit dem Ursprungs-Port 21 aus, dem bekannten Port für FTP-Verkehr.
`name ftpdata`	Benennt den Filter mit `ftpdata`.
`sport ftp-data`	Wählt Datenverkehr mit dem Ursprungs-Port 20 aus, dem bekannten Port für FTP-DatenVerkehr.
`class ftp`	Identifiziert die Klasse, zu der die Filter `ftpout` und `ftpdata` gehören, in diesem Fall `ftp`.

Siehe auch

- Informationen zum Definieren von Filtern finden Sie unter „So definieren Sie Filter in der IPQoS-Konfigurationsdatei" auf Seite 870.
- Informationen zum Definieren des Weiterleitungsverhaltens für den Datenverkehr von Anwendungen finden Sie unter „So konfigurieren Sie die Weiterleitung von Datenverkehr für Anwendungen in der IPQoS-Konfigurationsdatei" auf Seite 884.
- Informationen zur Konfiguration der Verkehrssteuerung mithilfe von Metermodulen finden Sie unter „So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei" auf Seite 887.
- Informationen zur Konfiguration des Flow Accounting finden Sie unter „So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei" auf Seite 875.

▼ So konfigurieren Sie die Weiterleitung von Datenverkehr für Anwendungen in der IPQoS-Konfigurationsdatei

Im nächsten Verfahren wird gezeigt, wie die Weiterleitung für den Datenverkehr von Anwendungen konfiguriert wird. In diesem Verfahren definieren Sie die Per-Hop-Behaviors für die Datenverkehrsklassen von Anwendungen, die eventuell eine niedrigere Prioritätsstufe als anderer Datenverkehr im Netzwerk haben. Mit dem folgenden Schritten wird die Datei `/var/ipqos/BigAPPS.qos` aus Beispiel 34–3 erweitert.

Bevor Sie beginnen Bei diesem Verfahren wird davon ausgegangen, dass Sie bereits eine IPQoS-Konfigurationsdatei erstellt und Klassen sowie Filter für die zu markierenden Anwendungen erstellt haben.

1. **Öffnen Sie die IPQoS-Konfigurationsdatei, die Sie für den Anwendungsserver erstellt haben, und suchen Sie das Ende der letzten** `filter`**-Klausel.**

   In der Datei `/var/ipqos/BigAPPS.qos` lautet der letzte Filter wie folgt:

```
 filter {
        name ftpdata
        sport ftp-data
        class ftp
    }
}
```

2. **Rufen Sie den Marker wie folgt auf:**

```
action {
    module dscpmk
    name markAF13
```

`module dscpmk`	Ruft das Markermodul `dscpmk` auf.
`name markAF13`	Benennt die `action`-Anweisung mit `markAF13`.

3. **Definieren Sie das Per-Hop-Behavior, das in einem E-Mail-Verkehrswert markiert werden soll.**

```
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
```

`global_stats FALSE`	Aktiviert die Erfassung von Statistiken für die `markAF13` Marker `action`-Anweisung. Da der Wert für `enable_stats FALSE` lautet, werden keine Statistiken erfasst.
`dscp_map{0–63:14}`	Weist den Paket-Headern der Datenverkehrklasse `smtp`, die momentan vom Marker verarbeitet werden, einen DSCP von `14` zu.
`next_action continue`	Gibt an, dass keine weitere Verarbeitung für Pakete der Datenverkehrsklasse `smtp` erforderlich ist. Diese Pakete können dann in den Netzwerkdatenfluss zurückkehren.

   Der DSCP `14` weist den Marker an, alle Einträge in der `dscp`-Map auf den Dezimalwert 14 (binär 001110) zu setzen. Der DSCP von `14` richtet das Per-Hop-Behavior AF13 ein. Der Marker markiert Pakete der Datenverkehrsklasse `smtp` mit dem DSCP `14` im DS-Feld.

AF13 weist allen Paketen mit einem DSCP von 14 eine high-drop-Prioritätsstufe zu. Da AF13 jedoch eine Class 1-Priorität sicherstellt, garantiert der Router abgehendem E-Mail-Verkehr dennoch hohe Priorität in der Warteschlange. Eine Liste der möglichen AF-Codepoints finden Sie in Tabelle 37–2.

4 **Fügen Sie eine Marker `action`-Anweisung hinzu, um ein Per-Hop-Behavior für den Network News-Datenverkehr zu definieren:**

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

`name markAF21`	Benennt die `action`-Anweisung mit `markAF21`.
`dscp_map{0–63:18}`	Weist den Paket-Headern der Datenverkehrklasse `nntp`, die momentan vom Marker verarbeitet werden, einen DSCP von 18 zu.

Der DSCP 18 weist den Marker an, alle Einträge in der `dscp`-Map auf den Dezimalwert 18 (binär 010010) zu setzen. Der DSCP von 18 richtet das Per-Hop-Behavior AF21 ein. Der Marker markiert Pakete der Datenverkehrsklasse `news` mit dem DSCP 18 im DS-Feld.

AF21 stellt sicher, dass alle Pakete mit dem DSCP 18 eine low-drop-Prioritätsstufe mit einer Class 2-Priorität erhalten. Somit ist die Wahrscheinlichkeit gering, dass Network News-Datenverkehr abgeworfen wird.

Siehe auch

- Informationen zum Hinzufügen von Konfigurationsinformationen für Webserver finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.
- Informationen zur Konfiguration der Verkehrssteuerung mithilfe von Metermodulen finden Sie unter „So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei“ auf Seite 887.
- Informationen zur Konfiguration des Flow Accounting finden Sie unter „So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei“ auf Seite 875.
- Informationen zur Konfiguration der Weiterleitungsverhalten auf einem Router finden Sie unter „So konfigurieren Sie einen Router in einem IPQoS-konformen Netzwerk“ auf Seite 890.
- Informationen zum Aktivieren der IPQoS-Konfigurationsdatei finden Sie unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module“ auf Seite 894.

▼ So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei

Zum Steuern der Rate, mit der ein bestimmter Verkehrswert in das Netzwerk freigegeben wird, müssen Sie Parameter für den Meter definieren. Sie können eines der beiden Metermodule `tokenmt` und `tswtclmt` in der IPQoS-Konfigurationsdatei verwenden.

Im folgenden Verfahren wird die IPQoS-Konfigurationsdatei für den Anwendungsserver aus Beispiel 34–3 erweitert. In diesem Verfahren konfigurieren Sie nicht nur den Meter, sondern auch zwei Markeraktionen, die in der `action`-Anweisung für den Meter aufgerufen werden.

Bevor Sie beginnen Bei diesen Schritten wird davon ausgegangen, dass Sie bereits eine Klasse sowie einen Filter für die Anwendung erstellt haben, deren Datenfluss gesteuert werden soll.

1. **Öffnen Sie die IPQoS-Konfigurationsdatei, die Sie für den Anwendungsserver erstellt haben.**

   Beginnen Sie in der Datei `/var/ipqos/BigAPPS.qos` unter der folgenden Markeraktion:

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

2. **Erstellen Sie eine Meter `action`-Anweisung, um eine Flusskontrolle für den Datenverkehr der `ftp`-Klasse einzurichten.**

```
action {
    module tokenmt
    name meterftp
```

`module tokenmt`	Ruft den Meter `tokenmt` auf.
`name meterftp`	Benennt die `action`-Anweisung mit `meterftp`.

3. **Fügen Sie Parameter hinzu, um die Rate des Meters zu konfigurieren.**

```
params {
       committed_rate 50000000
       committed_burst 50000000
```

`committed_rate 50000000`	Weist eine Übertragungsrate von 50.000.000 Bit/s für den Datenverkehr der `ftp`-Klasse zu.
`committed_burst 50000000`	Übernimmt eine Burst-Größe von 50.000.000 Bit für den Datenverkehr der `ftp`-Klasse.

Eine Beschreibung der `tokenmt`-Parameter finden Sie unter „Konfiguration von `tokenmt` als Two-Rate Meter“ auf Seite 911.

4 Fügen Sie Parameter hinzu, um die Prioritätsstufe der Datenverkehrskonformität zu konfigurieren:

```
    red_action markAF31
    green_action_name markAF22
    global_stats TRUE
    }
}
```

`red_action_name markAF31`	Gibt an, dass wenn der Verkehrswert der `ftp`-Klasse die Committed Rate überschreitet, Pakete an die `markAF31` Marker `action`-Anweisung gesendet werden.
`green_action_name markAF22`	Gibt an, dass wenn der Verkehrswert der `ftp`-Klasse der Committed Rate entspricht, Pakete an die action-Anweisung `markAF22` gesendet werden.
`global_stats TRUE`	Aktiviert die Erfassung der Messstatistiken für die `ftp`-Klasse.

Weitere Informationen zur Datenverkehrskonformität finden Sie unter „Metermodul“ auf Seite 910.

5 Fügen Sie eine Marker `action`-Anweisung hinzu, um ein Per-Hop-Behavior für nicht einen spezifikationsgerechten Verkehrswert der `ftp`-Klasse zuzuweisen.

```
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
```

`module dscpmk`	Ruft das Markermodul `dscpmk` auf.
`name markAF31`	Benennt die `action`-Anweisung mit `markAF31`.
`global_stats TRUE`	Aktiviert die Erfassung der Statistiken für die `ftp`-Klasse.
`dscp_map{0–63:26}`	Weist den Paket-Headern des Datenverkehr der `ftp`-Klasse einen DSCP von 26 zu, wenn dieser Datenverkehr die Committed Rate überschreitet.
`next_action continue`	Gibt an, dass keine weitere Verarbeitung für Pakete der Datenverkehrsklasse `ftp` erforderlich ist. Diese Pakete können dann in den Netzwerkdatenfluss zurückkehren.

Der DSCP `26` weist den Marker an, alle Einträge in der `dscp`-Map auf den Dezimalwert 26 (binär 011010) zu setzen. Der DSCP von `26` richtet das Per-Hop-Behavior AF31 ein. Der Marker markiert Pakete der Datenverkehrsklasse `ftp` mit dem DSCP `26` im DS-Feld.

AF31 stellt sicher, dass alle Pakete mit dem DSCP `26` eine low-drop-Prioritätsstufe mit einer Class 3-Priorität erhalten. Somit ist die Wahrscheinlichkeit gering, dass nicht spezifikationsgerechter FTP-Datenverkehr abgeworfen wird. Eine Liste der möglichen AF-Codepoints finden Sie in Tabelle 37–2.

6 Fügen Sie eine Marker `action`-Anweisung hinzu, um ein Per-Hop-Behavior für den `ftp`-Verkehrswert zuzuweisen, der der Committed Rate entspricht.

```
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

`name markAF22` — Benennt die Marker `action`-Anweisung mit `markAF22`.

`dscp_map{0–63:20}` — Weist den Paket-Headern des Datenverkehr der `ftp`-Klasse einen DSCP von `20` zu, wenn der `ftp`-Datenverkehr der Committed Rate entspricht.

Der DSCP `20` weist den Marker an, alle Einträge in der dscp-Map auf den Dezimalwert 20 (binär 010100) zu setzen. Der DSCP von `20` richtet das Per-Hop-Behavior AF22 ein. Der Marker markiert Pakete der Datenverkehrsklasse `ftp` mit dem DSCP `20` im DS-Feld.

AF22 stellt sicher, dass alle Pakete mit dem DSCP `20` eine medium-drop-Prioritätsstufe mit einer Class 2-Priorität erhalten. So wird für spezifikationsgerechtem FTP-Datenverkehr eine medium-drop-Prioritätsstufe im Vergleich zu anderen Datenströmen sichergestellt, die gleichzeitig vom PQoS-System freigegeben werden. Der Router weist Datenverkehrsklassen mit einer Class 1 medium-drop-Prioritätsstufe oder höher jedoch eine höhere Priorität bei der Weiterleitung zu. Eine Liste der möglichen AF-Codepoints finden Sie in Tabelle 37–2.

7 Fügen Sie die gerade für den Anwendungsserver erstellten DSCPs zu den entsprechenden Dateien auf dem Diffserv-Router hinzu.

Siehe auch

- Informationen zum Aktivieren der IPQoS-Konfigurationsdatei finden Sie unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module“ auf Seite 894.
- Informationen zum Hinzufügen von Konfigurationsinformationen für Webserver finden Sie unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.

- Informationen zur Konfiguration des Flow Accounting finden Sie unter „So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei“ auf Seite 875.
- Informationen zur Konfiguration der Weiterleitungsverhalten auf einem Router finden Sie unter „So konfigurieren Sie einen Router in einem IPQoS-konformen Netzwerk“ auf Seite 890.

Bereitstellen von Differentiated Services auf einem Router

Um echte Differentiated Services bereitzustellen, müssen Sie einen Diffserv-konformen Router in Ihre Netzwerktopologie aufnehmen. Eine Beschreibung hierzu finden Sie unter „Hardware-Strategien für das Diffserv-Netzwerk“ auf Seite 842. Die tatsächlichen Schritte zur Konfiguration von Diffserv auf einem Router und zum Aktualisieren der Routerdateien sprengen jedoch den Umfang dieses Handbuchs.

Daher finden Sie hier nur allgemeine Schritte zur Koordinierung der Weiterleitungsinformationen zwischen verschiedenen IPQoS-konformen Systemen im Netzwerk und dem Diffserv-Router.

▼ So konfigurieren Sie einen Router in einem IPQoS-konformen Netzwerk

Im folgenden Verfahren wird die in Abbildung 33–4 vorgestellte Topologie als Beispiel verwendet.

Bevor Sie beginnen Im folgenden Verfahren wird davon ausgegangen, dass die IPQoS-Systeme in Ihrem Netzwerk bereits konfiguriert sind, da Sie die vorherigen Aufgaben in diesem Kapitel ausgeführt haben.

1 Erstellen Sie eine Übersicht der Konfigurationsdateien aller IPQoS-konformen Systeme in Ihrem Netzwerk.

2 Identifizieren Sie jeden Codepoint, der in den verschiedenen QoS-Richtlinien verwendet wird.

Erstellen Sie eine Liste der Codepoints sowie der Systeme und Klassen, für die die Codepoints gelten. Die folgende Tabelle zeigt Bereiche, in denen Sie eventuell den gleichen Codepoint verwenden. Diese Vorgehensweise ist akzeptabel. Sie sollten jedoch weitere Kriterien in der IPQoS-Konfigurationsdatei bereitstellen, z. B. einen Selektor für die `Prioritätsstufe`, um die Prioritätsstufe identisch markierter Klassen zu bestimmen.

Für das in den Verfahren dieses Kapitels verwendeten Beispielnetzwerk können Sie die folgende Codepoint-Tabelle erstellen.

System	Klasse	PHB	DS Codepoint
Goldweb	video	EF	46 (101110)
Goldweb	goldweb	AF11	10 (001010)
Userweb	webout	AF12	12 (001100)
BigAPPS	smtp	AF13	14 (001110)
BigAPPS	news	AF18	18 (010010)
BigAPPS	ftp-spezifikationsgerechter Datenverkehr	AF22	20 (010100)
BigAPPS	ftp-nicht spezifikationsgerechter Datenverkehr	AF31	26 (011010)

3 Fügen Sie die Codepoints aus den IPQoS-Konfigurationsdateien Ihres Netzwerks zu den entsprechenden Dateien auf dem Diffserv-Router hinzu.

Die von Ihnen angegebenen Codepoints helfen bei der Konfiguration des Diffserv-Scheduling-Mechanismus des Routers. Weitere Hinweise entnehmen Sie bitte der Dokumentation des Router-Herstellers sowie dessen Websites.

KAPITEL 35

Starten und Verwalten des IPQoS (Aufgaben)

Dieses Kapitel enthält Aufgaben zum Aktivieren einer IPQoS-Konfigurationsdatei sowie zum Protokollieren von IPQoS-bezogenen Ereignissen. Es umfasst die folgenden Themen:

- „Verwalten des IPQoS (Übersicht der Schritte)" auf Seite 893
- „Übernehmen einer IPQoS-Konfiguration" auf Seite 894
- „Aktivieren von `syslog` zum Protokollieren von IPQoS-Nachrichten" auf Seite 896
- „Fehlerbehebung mit IPQoS-Fehlermeldungen" auf Seite 897

Verwalten des IPQoS (Übersicht der Schritte)

In diesem Abschnitt sind Aufgaben zum Starten und Verwalten des IPQoS auf einem Oracle Solaris-System beschrieben. Bevor Sie diese Aufgaben durchführen können, müssen Sie eine vollständige IPQoS-Konfigurationsdatei erstellt haben. Informationen hierzu finden Sie unter „Definieren einer QoS-Richtlinie in der IPQoS-Konfigurationsdatei (Übersicht der Schritte)" auf Seite 863.

In der folgenden Tabelle werden diese Aufgaben aufgeführt und beschrieben. Außerdem enthält die Tabelle Links zu den Abschnitten, in denen beschrieben ist, wie diese Aufgaben ausgeführt werden.

Aufgabe	Beschreibung	Siehe
1. Konfiguration von IPQoS auf einem System.	Geben Sie den Befehl `ipqosconf` ein, um die IPQoS-Konfigurationsdatei auf einem System zu aktivieren.	„So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module" auf Seite 894

Aufgabe	Beschreibung	Siehe
2. Konfiguration der Oracle Solaris-Startskripten, so dass sie die geprüfte IPQoS-Konfigurationsdatei nach jedem Systemstart anwenden.	Stellen Sie sicher, dass die IPQoS-Konfiguration bei jedem Systemstart übernommen wird.	„So stellen Sie sicher, dass die IPQoS-Konfiguration bei jedem Systemstart übernommen wird" auf Seite 895.
3. Konfiguration von `syslog` zum Protokollieren für IPQoS.	Fügen Sie einen Eintrag hinzu, um `syslog` zum Protokollieren von IPQoS-Nachrichten zu aktivieren.	„So aktivieren Sie die Protokollierung von IPQoS-Nachrichten während des Bootens" auf Seite 896.
4. Bereinigen aller eventuell aufgetretenen IPQoS-Probleme.	Beheben Sie alle eventuell aufgetretenen IPQoS-Probleme anhand der Fehlermeldungen.	Lesen Sie dazu die Fehlermeldungen in Tabelle 35–1.

Übernehmen einer IPQoS-Konfiguration

Mit dem Befehl `ipqosconf` aktivieren und ändern Sie eine IPQoS-Konfiguration.

▼ So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module

Geben Sie den Befehl `ipqosconf` ein, um die IPQoS-Konfigurationsdatei einzulesen und um die IPQoS-Module im UNIX-Kernel zu konfigurieren. Im folgenden Verfahren wird die unter `Creating IPQoS Configuration Files for Web Servers` erstellte Datei „Erstellen von IPQoS-Konfigurationsdateien für Webserver" auf Seite 866 als Beispiel verwendet. Ausführliche Informationen finden Sie in der Manpage `ipqosconf`(1M).

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser bei dem IPQ-konformen System an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2. **Übernehmen Sie die neue Konfiguration.**

   ```
   # /usr/sbin/ipqosconf -a/var/ipqos/Goldweb.qos
   ```

   `ipqosconf` schreibt die Informationen aus der angegebenen IPQoS-Konfigurationsdatei in die IPQoS-Module im Oracle Solaris-Kernel. In diesem Beispiel werden die Inhalte der Datei `/var/ipqos/Goldweb.qos` für den aktuellen Oracle Solaris-Kernel übernommen.

Hinweis – Wenn Sie eine IPQoS-Konfigurationsdatei mit der Option `-a` übernehmen, gelten die Aktionen in der Datei nur für die aktuelle Sitzung.

---

3 **Testen und bereinigen Sie die neue IPQoS-Konfiguration.**

Verwenden Sie UNIX-Serviceprogramme, um das IPQo-Verhalten zu verfolgen und erfassen Sie Statistiken zu Ihrer IPQoS-Implementierung. Diese Informationen helfen Ihnen festzustellen, ob die Konfiguration gemäß den Erwartungen funktioniert.

Siehe auch

- Informationen zum Anzeigen von Statistiken zu den IPQoS-Modulen finden Sie unter „Erfassen statistischer Informationen" auf Seite 904.
- Informationen zum Protokollieren der `ipqosconf`-Nachrichten finden Sie unter „Aktivieren von `syslog` zum Protokollieren von IPQoS-Nachrichten" auf Seite 896.
- Informationen, wie Sie sicherstellen, dass die aktuelle IPQoS-Konfiguration bei jedem Systemstart übernommen wird, finden Sie unter „So stellen Sie sicher, dass die IPQoS-Konfiguration bei jedem Systemstart übernommen wird" auf Seite 895.

▼ So stellen Sie sicher, dass die IPQoS-Konfiguration bei jedem Systemstart übernommen wird

Sie müssen explizit konfigurieren, dass eine IPQoS-Konfiguration bei jedem Neustart übernommen wird. Andernfalls gilt die aktuelle Konfiguration nur für die aktuelle Sitzung. Wenn IPQoS korrekt auf einem System arbeitet, führen Sie die folgenden Schritte aus, um sicherzustellen, dass die Konfiguration bei jedem Neustart übernommen wird.

1 **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser bei dem IPQ-konformen System an.**

Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)" in *System Administration Guide: Basic Administration*.

2 **Prüfen Sie auf das Vorhandensein einer IPQoS-Konfiguration in den Kernel-Modulen.**

```
# ipqosconf -l
```

Wenn eine Konfiguration vorhanden ist, zeigt der Befehl `ipqosconf` die Konfiguration auf dem Bildschirm an. Wird keine Ausgabe angezeigt, übernehmen Sie die Konfiguration gemäß der Beschreibung unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module" auf Seite 894.

3. **Stellen Sie sicher, dass die vorhandene IPQoS-Konfiguration bei jedem Neustart des IPQoS-Systems übernommen wird.**

```
# /usr/sbin/ipqosconf -c
```

Die Option `-c` sorgt dafür, dass die aktuelle IPQoS-Konfiguration in der Boot-Konfigurationsdatei `/etc/inet/ipqosinit.conf` vorhanden ist.

Aktivieren von `syslog` zum Protokollieren von IPQoS-Nachrichten

Zum Aufzeichnen von Nachrichten, die beim Booten von IPQoS erzeugt werden, müssen Sie die Datei `/etc/syslog.conf` wie im Folgenden gezeigt ändern.

▼ So aktivieren Sie die Protokollierung von IPQoS-Nachrichten während des Bootens

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser bei dem IPQ-konformen System an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2. **Öffnen Sie die Datei** `/etc/syslog.conf`**.**

3. **Fügen Sie den folgenden Text als letzten Eintrag in die Datei ein.**

```
user.info                 /var/adm/messages
```

   Verwenden Sie Tabulatoren anstelle von Leerzeichen zwischen den Spalten.

   Der Eintrag protokolliert alle Nachrichten, die von IPQoS beim Booten erzeugt werden, in der Datei `/var/adm/messages`.

4. **Booten Sie das System neu, um die Nachrichten zu übernehmen.**

Beispiel 35–1 IPQoS-Ausgabe von `/var/adm/messages`

Wenn Sie die `/var/adm/messages` nach einem Systemneustart anzeigen, könnte die Ausgabe die folgenden protokollierten IPQoS-Nachrichten enthalten.

```
May 14 10:44:33 ipqos-14 ipqosconf: [ID 815575 user.info]
 New configuration applied.
May 14 10:44:46 ipqos-14 ipqosconf: [ID 469457 user.info]
```

```
Current configuration saved to init file.
May 14 10:44:55 ipqos-14 ipqosconf: [ID 435810 user.info]
Configuration flushed.
```

Eventuell werden auch die folgenden IPQoS-Fehlermeldungen in der `/var/adm/messages`-Datei des IPQoS-Systems angezeigt.

```
May 14 10:56:47 ipqos-14 ipqosconf: [ID 123217 user.error]
 Missing/Invalid config file fmt_version.
May 14 10:58:19 ipqos-14 ipqosconf: [ID 671991 user.error]
No ipgpc action defined.
```

Eine Beschreibung dieser Fehlermeldungen finden Sie in Tabelle 35–1.

Fehlerbehebung mit IPQoS-Fehlermeldungen

Dieser Abschnitt enthält von IPQoS erzeugte Fehlermeldungen sowie mögliche Abhilfemaßnahmen.

TABELLE 35–1 IPQoS-Fehlermeldungen

Fehlermeldung	Beschreibung	Lösung
`Unbestimmte Aktion in Parameter` *Parametername* `Aktion` *Aktionsname*	Der in *Parametername* angegebene Aktionsname existiert nicht in der IPQoS-Konfigurationsdatei.	Erstellen Sie die Aktion oder verweisen Sie auf eine andere vorhandene Aktion in dem Parameter.
`Aktion` *Aktionsname* `ist am Zyklus beteiligt.`	In der IPQoS-Konfigurationsdatei ist *Aktionsname* Teil eines Aktionszyklus, der laut IPQoS nicht zulässig ist.	Ermitteln Sie den Aktionszyklus. Dann entfernen Sie einen der zyklischen Verweise aus der IPQoS-Konfigurationsdatei.
`Aktion` *Aktionsname* `wird von keiner anderen Aktion referenziert`	Eine nicht-`ipgpc`-Aktionsdefinition wurde von keiner anderen in der IPQoS-Konfiguration definierten Aktionen referenziert. Dies ist laut IPQoS nicht gestattet.	Entfernen Sie die nicht referenzierte Aktion. Alternativ sorgen Sie dafür, dass eine andere Aktionsreferenz die derzeit nicht referenzierte Aktion referenziert.
`Fehlende/ungültige Konfigurationsdatei fmt_version`	Das Format der Konfigurationsdatei ist nicht als erster Eintrag der Datei angegeben. Dies ist jedoch eine Voraussetzung für IPQoS.	Fügen Sie die Formatversion gemäß den Angaben unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868 hinzu.
`Nicht unterstützte Konfigurationsdatei-Formatversion`	Die in der Konfigurationsdatei angegebene Formatversion wird nicht von IPQoS unterstützt.	Ändern Sie die Formatversion zu `fmt_version 1.0`. Diese Formatversion ist zum Ausführen von Solaris 9 9/02 und höheren Versionen von IPQoS erforderlich.
`Keine ipgpc-Aktion definiert.`	Sie haben keine Aktion für den `ipgpc`-Classifier in der Konfigurationsdatei definiert. Dies ist jedoch eine Voraussetzung für IPQoS.	Definieren Sie eine Aktion für `ipgpc` gemäß den Angaben unter „So erstellen Sie eine IPQoS-Konfigurationsdatei und definieren Datenverkehrsklassen“ auf Seite 868.

TABELLE 35–1 IPQoS-Fehlermeldungen *(Fortsetzung)*

Fehlermeldung	Beschreibung	Lösung
`Es kann keine Null-Konfiguration vorgenommen werden`	Als Sie `ipqosconf -c` zur Bestätigung einer Konfiguration ausführen wollten, war diese Rekonfiguration leer. Dies ist laut IPQoS nicht zulässig.	Achten Sie darauf, eine Konfigurationsdatei zu übernehmen, bevor Sie versuchen, eine Konfiguration zu bestätigen. Anweisungen hierzu finden Sie unter „So übernehmen Sie eine neue Konfigurationen für die IPQoS-Kernel-Module“ auf Seite 894.
`Ungültige CIDR-Maske Zeile` *Zeilennummer*	In der Konfigurationsdatei haben Sie eine CIDR-Maske als Teil der IP-Adresse verwendet, die sich außerhalb des gültigen Bereichs für IP-Adressen befindet.	Ändern Sie den Wert der Maske so, dass er sich im Bereich von 1–32 für IPv4 und 1–128 für IPv6 befindet.
`Adressmasken sind unzulässig für Hostnamen Zeile` *Zeilennummer*	In der Konfigurationsdatei haben Sie eine CIDR-Maske für einen Hostnamen definiert, der in IPQoS nicht zulässig ist.	Entfernen Sie die Maske oder ändern Sie den Hostnamen zu einer IP-Adresse.
`Ungültiger Modulname, Zeile` *Zeilennummer*	In der Konfigurationsdatei ist der von Ihnen in einer action-Anweisung angegebenen Modulname ungültig.	Prüfen Sie die richtige Schreibweise des Modulnamens. Eine Liste der IPQoS-Module finden Sie unter Tabelle 37–5.
`ipgpc-Aktion weist falschen Namen auf, Zeile` *Zeilennummer*	Der Name, den Sie der `ipgpc`-Aktion in der Konfigurationsdatei gegeben haben, ist nicht der erforderliche `ipgpc.classify`-Name.	Benennen Sie die Aktion `ipgpc.classify` um.
`Zweite Parameterklausel nicht unterstützt, Zeile` *Zeilennummer*	In der Konfigurationsdatei haben Sie zwei Parameterklauseln für eine Aktion angegeben. Dies ist laut IPQoS nicht zulässig.	Kombinieren Sie alle Parameter für die Aktion in einer Parameterklausel.
`Gleichnamige Aktion`	In der Konfigurationsdatei haben zwei Aktionen den gleichen Namen.	Benennen Sie eine der Aktionen um, oder löschen Sie sie.
`Gleichnamiger Filter/Klasse in Aktion` *Aktionsname*	Sie haben zwei Filtern oder zwei Klassen in der gleichen Aktion denselben Namen gegeben. Dies ist in der IPQoS-Konfigurationsdatei nicht zulässig.	Benennen Sie einen der Filter bzw. eine der Klassen um, oder löschen Sie sie.
`Unbestimmte Klasse in Filter` *Filtername* `Aktion` *Aktionsname*	In der Konfigurationsdatei verweist der Filter auf eine Klasse, die nicht in der Aktion definiert ist.	Erstellen Sie die Klasse oder ändern Sie den Filterverweis auf eine bereits existierende Klasse.
`Unbestimmte Aktion in Klasse` *Klassenname* `Aktion` *Aktionsname*	Die Klasse verweist auf eine Aktion, die nicht in der Konfigurationsdatei definiert ist.	Erstellen Sie die Aktion oder ändern Sie den Verweis auf eine bereits existierende Aktion.

TABELLE 35–1 IPQoS-Fehlermeldungen *(Fortsetzung)*

Fehlermeldung	Beschreibung	Lösung
`Ungültige Parameter für Aktion` *Aktionsname*	Einer der Parameter in der Konfigurationsdatei ist ungültig.	Lesen Sie den Moduleintrag unter „IPQoS-Architektur und das Diffserv-Modell" auf Seite 907 für das Modul, das von der angegebenen Aktion aufgerufen wird. Alternativ lesen Sie die Manpage `ipqosconf`(1M).
`Obligatorischer Parameter fehlt für Aktion` *Aktionsname*	Ein für die Aktion erforderlicher Parameter ist in der Konfigurationsdatei nicht definiert.	Lesen Sie den Moduleintrag unter „IPQoS-Architektur und das Diffserv-Modell" auf Seite 907 für das Modul, das von der angegebenen Aktion aufgerufen wird. Alternativ lesen Sie die Manpage `ipqosconf`(1M).
`In ipgpc wurde die max. Klassenanzahl erreicht`	Sie haben mehr Klassen als zulässig in der `ipgpc`-Aktion der IPQoS-Konfigurationsdatei angegeben. Die maximal zulässige Anzahl beträgt 10007.	Prüfen Sie die Konfigurationsdatei und entfernen Sie unnötige Klassen. Alternativ heben Sie die maximale Klassenanzahl an, indem Sie der `/etc/system`-Datei den Eintrag `ipgpc_max_classes`*Anzahl-an-Klassen* hinzufügen.
`In der Aktion ipgpc wurde die max. Filteranzahl erreicht`	Sie haben mehr Filter als zulässig in der `ipgpc`-Aktion der IPQoS-Konfigurationsdatei angegeben. Die maximal zulässige Anzahl beträgt 10007.	Prüfen Sie die Konfigurationsdatei und entfernen Sie unnötige Filter. Alternativ heben Sie die maximale Filteranzahl an, indem Sie der `/etc/system`-Datei den Eintrag `ipgpc_max_filters` *Anzahl-an-Filtern* hinzufügen.
`Ungültige/fehlende Parameter für Filter` *Filtername* `in Aktion ipgpc`	In der Konfigurationsdatei weist der Filter *Filtername* einen ungültigen oder fehlenden Parameter auf.	Eine Liste der gültigen Parameter finden Sie in der Manpage `ipqosconf`(1M).
`Name darf nicht mit '!' beginnen, Zeile` *Zeilennummer*	Sie haben eine Aktion, ein Filter oder einen Klassennamen mit einem Ausrufezeichen (!) begonnen, was in IPQoS-Dateien nicht zulässig ist.	Entfernen Sie das Ausrufezeichen oder benennen Sie die Aktion, Klasse bzw. den Filter um.
`Name überschreitet maximale Länge Zeile` *Zeilennummer*	Sie haben einen Namen für eine Aktion, eine Klasse oder einen Filter in der Konfigurationsdatei definiert, der die maximale Länge von 23 Zeichen überschreitet.	Weisen Sie der Aktion, der Klasse oder dem Filter einen kürzeren Namen zu.
`Array-Deklaration Zeile` *Zeilennummer* `ist ungültig`	In der Konfigurationsdatei ist die Array-Deklaration für den Parameter in der Zeile *Zeilennummer* ungültig.	Die korrekte Syntax der Array-Deklaration, die von der `action`-Anweisung mit dem ungültigen Array aufgerufen wird, finden Sie unter „IPQoS-Architektur und das Diffserv-Modell" auf Seite 907. Alternativ lesen Sie die Manpage `ipqosconf`(1M).
`Zeichenkette in Anführungszeichen überschreitet Zeile, Zeile ,` *Zeilennummer*	Diese Zeichenkette weist keine Beendigungs-Anführungszeichen in der gleichen Zeile auf. Dies ist in der Konfigurationsdatei erforderlich.	Achten Sie darauf, dass die entsprechende Zeichenkette auf einer Zeile in der Konfigurationsdatei beginnt und endet.

TABELLE 35–1 IPQoS-Fehlermeldungen *(Fortsetzung)*

Fehlermeldung	Beschreibung	Lösung
`Ungültiger Wert, Zeile` *Zeilennummer*	Der in *Zeilennummer* der Konfigurationsdatei angegebene Wert wird für den Parameter nicht unterstützt.	Gültige Werte für das Modul, das von der `action`-Anweisung aufgerufen wird, entnehmen Sie der Modulbeschreibung unter „IPQoS-Architektur und das Diffserv-Modell" auf Seite 907. Alternativ lesen Sie die Manpage `ipqosconf`(1M).
`Nicht erkannter Wert, Zeile` *Zeilennummer*	Der Wert in *Zeilennummer* der Konfigurationsdatei ist kein unterstützter Aufzählungswert für diesen Parameter.	Prüfen Sie, ob der Aufzählungswert für diesen Parameter korrekt ist. Eine Beschreibung des Moduls, das von der `action`-Anweisung mit der nicht erkannten Zeilennummer aufgerufen wurde, finden Sie unter „IPQoS-Architektur und das Diffserv-Modell" auf Seite 907. Alternativ lesen Sie die Manpage `ipqosconf`(1M).
`Falsch formatierte Werteliste Zeile` *Zeilennummer*	Die in *Zeilennummer* der Konfigurationsdatei angegebene Aufzählung entspricht nicht der Spezifikationssyntax.	Die korrekte Syntax für das Modul, das von der `action`-Anweisung mit der falsch formatierten Werteliste aufgerufen wurde, entnehmen Sie der Modulbeschreibung unter „IPQoS-Architektur und das Diffserv-Modell" auf Seite 907. Alternativ lesen Sie die Manpage `ipqosconf`(1M).
`Doppelter Parameter Zeile` *Zeilennummer*	Ein doppelter Parameter wurde in *Zeilennummer* angegeben. Dies ist in der Konfigurationsdatei nicht zulässig.	Entfernen Sie einen der doppelten Parameter.
`Ungültiger Aktionsname Zeile` *Zeilennummer*	Sie haben der Aktion in *Zeilennummer* der Konfigurationsdatei einen Namen gegeben, der den vordefinierten Namen „continue" oder „drop" verwendet."	Benennen Sie die Aktion um, so dass sie keinen vordefinierten Namen verwendet.
`Fehler bei Auflösung des Ursprungs-/Zielhostnamens für Filter in Zeile` *Zeilennummer*`, Filter wird ignoriert`	`ipqosconf` konnte die Ursprungs- oder Zieladresse nicht auflösen, die für den angegebenen Filter in der Konfigurationsdatei definiert wurde. Aus diesem Grund wird der Filter ignoriert.	Wenn der Filter wichtig ist, versuchen Sie die Konfiguration zu einem späteren Zeitpunkt zu übernehmen.
`Inkompatible Adressversion Zeile` *Zeilennummer*	Die IP-Version der Adresse in *Zeilennummer* ist inkompatibel mit der Version einer zuvor angegebenen IP-Adresse oder dem Parameter `ip_version`.	Ändern Sie die beiden widersprüchlichen Einträge, so dass sie kompatibel sind.
`Aktion in Zeile` *Zeilennummer* `hat den Namen wie die aktuell installierte Aktion, gilt aber für ein anderes Modul`	Sie versuchten, das Modul einer Aktion zu ändern, das bereits in der IPQoS-Konfiguration des Systems vorhanden ist. Dies ist nicht zulässig.	Leeren Sie die aktuelle Konfiguration, bevor Sie die neue Konfiguration übernehmen.

KAPITEL 36

Verwenden von Flow Accounting und Erfassen von Statistiken (Aufgaben)

In diesem Kapitel wird beschrieben, wie Sie Informationen zum Accounting und Statistiken zum Datenverkehr beziehen, der von einem IPQoS-System verarbeitet wird. Folgende Themen werden behandelt:

- „Einrichten des Flow Accounting (Übersicht der Schritte)" auf Seite 901
- „Aufzeichnen von Informationen zu Verkehrswerten" auf Seite 902
- „Erfassen statistischer Informationen" auf Seite 904

Einrichten des Flow Accounting (Übersicht der Schritte)

Die folgende Tabelle enthält eine Liste der allgemeinen Aufgaben zum Beziehen von Informationen zu den Verkehrswerten mithilfe des `flowacct`-Moduls. Die Tabelle enthält Links zu den Verfahren zur Ausführung dieser Aufgaben.

Aufgabe	Beschreibung	Siehe
1. Erstellen einer Datei zur Aufnahme der Accounting-Informationen für Verkehrswerte.	Geben Sie den Befehl `acctadm` ein, um eine Datei zu erstellen, in der die Ergebnisse der Verarbeitung durch `flowacct` aufgenommen werden.	„So erstellen Sie eineDatei für die Flow Accounting-Daten" auf Seite 902
2. Definieren der `flowacct`-Parameter in der IPQoS-Konfigurationsdatei.	Definieren Sie Werte für die Parameter `timer`, `timeout` und `max_limit`.	„So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei" auf Seite 875

Aufzeichnen von Informationen zu Verkehrswerten

Mit dem IPQoS-Modul `flowacct` können Sie Informationen zu Verkehrswerten sammeln. Beispielsweise können Sie Informationen zu den Ursprungs- und Zieladressen, der Anzahl an Paketen in einem Datenfluss und ähnliche Daten erfassen. Dieses Sammeln und Aufzeichnen von Informationen zu Datenströmen wird als *Flow Accounting* bezeichnet.

Die Ergebnisse des Flow Accounting von Datenverkehr einer bestimmten Klasse wird in einer Tabelle mit *Flow-Datensätzen* aufgezeichnet. Jeder Flow-Datensatz enthält eine Reihe von Attributen. Diese Attribute enthalten Daten zu den Verkehrswerten einer bestimmten Klasse über einen bestimmten Zeitraum. Eine Liste der `flowacct`-Attribute finden Sie in Tabelle 37–4.

Das Flow Accounting eignet sich besonders zur Rechnungsstellung für Kunden gemäß den Definitionen in ihren Service-Level Agreements (SLAs). Sie können das Flow Accounting auch zum Beziehen von Flussstatistiken für entscheidende Anwendungen verwenden. In diesem Abschnitt wird beschrieben, wie Sie das Modul `flowacct` mit der Extended Accounting-Funktion von Oracle Solaris verwenden, um Daten zu Verkehrswerten zu beziehen.

Neben den Informationen in diesem Kapitel können Sie in den folgenden Quellen nachlesen:

- Informationen zum Erstellen einer action-Anweisung für das `flowacct`-Modul in der IPQoS-Konfigurationsdatei finden Sie unter „So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei“ auf Seite 887.
- Informationen zur Funktionsweise des `flowacct`-Moduls finden Sie unter „Classifier-Modul“ auf Seite 907.
- Technische Informationen finden Sie in der Manpage `flowacct`(7ipp).

▼ So erstellen Sie eineDatei für die Flow Accounting-Daten

Bevor Sie eine `flowacct`-Aktion zur IPQoS-Konfigurationsdatei hinzufügen, müssen Sie eine Datei für die Flow-Datensätze des `flowacct`-Moduls anlegen. Dafür verwenden Sie den Befehl `acctadm.` `acctadm` kann entweder allgemeine Attribute oder erweiterte Attribute in der Datei aufzeichnen. Eine Liste der `flowacct`-Attribute finden Sie in Tabelle 37–4. Ausführliche Informationen zum Befehl `acctadm` finden Sie in der Manpage `acctadm(1M)`.

1. **Nehmen Sie die Rolle eines Primäradministrators an, oder melden Sie sich als Superuser bei dem IPQ-konformen System an.**

   Die Rolle des Primäradministrators enthält das Primary Administrator-Profil. Informationen zum Erstellen von Rollen und Zuweisen von Rollen zu Benutzern finden Sie in Kapitel 2, „Working With the Solaris Management Console (Tasks)“ in *System Administration Guide: Basic Administration*.

2 Erstellen Sie eine allgemeine Flow Accounting-Datei.

Im folgenden Beispiel wird gezeigt, wie Sie eine allgemeine Flow Accounting-Datei für den Premium-Webserver erstellen, der in Beispiel 34–1 konfiguriert wurde.

```
# /usr/sbin/acctadm -e basic -f /var/ipqos/goldweb/account.info flow
```

`acctadm -e` — Ruft `acctadm` mit der Option `-e` auf. Die Option `-e` ermöglicht, dass weitere Argumente eingegeben werden können.

`basic` — Gibt an, dass nur Daten für die acht allgemeinen `flowacct`-Attribute in der Datei aufgezeichnet werden.

`/var/ipqos/goldweb/account.info` — Der vollständig qualifizierte Pfad zu der Datei, in der die Flow-Datensätze des `flowacct` -Moduls aufgezeichnet werden.

`flow` — Weist `acctadm` an, dass Flow Accounting zu aktivieren.

3 Zeigen Sie Informationen zum Flow Accounting auf dem IPQoS-System an, indem Sie den Befehl `acctadm` ohne weitere Argumente eingeben.

`acctadm` erzeugt die folgende Ausgabe:

```
Task accounting: inactive
       Task accounting file: none
     Tracked task resources: none
   Untracked task resources: extended
         Process accounting: inactive
    Process accounting file: none
  Tracked process resources: none
Untracked process resources: extended,host,mstate
            Flow accounting: active
       Flow accounting file: /var/ipqos/goldweb/account.info
     Tracked flow resources: basic
   Untracked flow resources: dsfield,ctime,lseen,projid,uid
```

Alle Einträge außer den letzten vier werden für die Funktion Solaris Resource Manager verwendet. In der folgenden Tabelle werden die speziell für IPQoS geltenden Einträge beschrieben.

Eintrag	Beschreibung
`Flow accounting: active`	Gibt an, dass das Flow Accounting aktiviert ist.
`Flow accounting file: /var/ipqos/goldweb/account.info`	Gibt den Namen der aktuellen Flow Accounting-Datei an.
`Tracked flow resources: basic`	Gibt an, dass nur allgemeine Datenflussattribute aufgezeichnet werden.

Eintrag	Beschreibung
`Untracked flow resources: dsfield,ctime,lseen,projid,uid`	Erstellt eine Liste der `flowacct`-Attribute, die nicht in der Datei aufgezeichnet werden.

4. **(Optional) Fügen Sie erweiterte Attribute zur Accounting-Datei hinzu.**

```
# acctadm -e extended -f /var/ipqos/goldweb/account.info flow
```

5. **(Optional) Kehren Sie zur Aufzeichnung nur der allgemeinen Attribute in der Accounting-Datei zurück.**

```
# acctadm -d extended -e basic -f /var/ipqos/goldweb/account.info
```

Die Option `-d` deaktiviert das Extended Accounting.

6. **Zeigen Sie den Inhalt einer Flow Accounting-Datei an.**

Anweisungen zum Anzeigen des Inhalts einer Flow Accounting-Datei finden Sie unter „Perl-Schnittstelle für libexacct“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

Siehe auch

- Ausführliche Informationen zum Extended Accounting finden Sie in Kapitel 4, „Einführung in das Extended Accounting“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.
- Informationen zum Definieren der `flowacct`-Parameter in der IPQoS-Konfigurationsdatei finden Sie unter „So aktivieren Sie das Accounting für eine Klasse in der IPQoS-Konfigurationsdatei“ auf Seite 875.
- Informationen zum Drucken der Daten in der Datei, die mit dem Befehl `acctadm` erstellt wurde, finden Sie in „Perl-Schnittstelle für libexacct“ in *Systemverwaltungshandbuch: Oracle Solaris Container – Ressourcenverwaltung und Solaris Zones*.

Erfassen statistischer Informationen

Mit dem Befehl `kstat` können Sie Statistiken zu dem IPQoS-Modulen erzeugen. Verwenden Sie die folgende Syntax:

`/bin/kstat -m` *ipqos-module-name*

Sie können jeden gültigen IPQoS-Modulnamen angeben. Eine Liste gültiger Namen finden Sie in Tabelle 37–5. Um beispielsweise Statistiken anzuzeigen, die von dem `dscpmk`-Marker erzeugt wurden, geben Sie den folgenden `kstat`-Befehl ein:

```
/bin/kstat -m dscpmk
```

Technische Informationen finden Sie in der Manpage `kstat`(1M).

BEISPIEL 36–1 `kstat`-Statistiken für IPQoS

Im Folgenden finden Sie ein Beispiel mögliche Ergebnisse des Befehls `kstat` zum Beziehen von Statistiken zum `flowacct`-Modul.

```
# kstat -m flowacct
module: flowacct                        instance: 3
name:   Flowacct statistics             class:    flacct
        bytes_in_tbl                    84
        crtime                          345728.504106363
        epackets                        0
        flows_in_tbl                    1
        nbytes                          84
        npackets                        1
        snaptime                        345774.031843301
        usedmem                         256
```

`class: flacct` Gibt den Namen der Klasse an, zu dem der Verkehrswert gehört; in diesem Fall `flacct`.

`bytes_in_tbl` Die Gesamtzahl an Byte in der Flow-Tabelle. Gesamtzahl an Byte ist die Summe der Byte aller Flow-Datensätze, die derzeit in der Flow-Tabelle aufgezeichnet sind. Die Gesamtanzahl der Bytes für diese Flow-Tabelle ist 84. Wenn in der Tabelle keine Flows vorhanden sind, ist der Wert für `bytes_in_tbl` gleich 0.

`crtime` Die letzte Uhrzeit, zu der eine `kstat`-Ausgabe erzeugt wurde.

`epackets` Die Anzahl an Paketen, die während der Verarbeitung zu einem Fehler führten, in diesem Beispiel 0.

`flows_in_tbl` Anzahl der Flow-Datensätze in der Flow-Tabelle (in diesem Beispiel 1). Wenn in der Tabelle keine Datensätze vorhanden sind, ist der Wert für `flows_in_tbl` gleich 0.

`nbytes` Die Gesamtzahl an Byte, die von dieser Instanz der `flowacct`-Aktion erfasst wurden, in diesem Beispiel 84. Dieser Wert umfasst die Byte, die derzeit in der Flow-Tabelle vorhanden sind. Dieser Wert schließt darüber hinaus alle Byte ein, für die ein Timeout aufgetreten ist und die nicht länger in der Flow-Tabelle vorhanden sind.

`npackets` Die Gesamtzahl an Paketen, die von dieser Instanz der `flowacct`-Aktion erfasst wurden, in diesem Beispiel 1. `npackets` umfasst auch die Pakete, die derzeit in der Flow-Tabelle vorhanden sind. `npackets` umfasst auch Pakete, für die ein Timeout aufgetreten ist und die nicht mehr in der Flow-Tabelle vorhanden sind.

`usedmem` Byte im Hauptspeicher, die von der Flow-Tabelle verwendet werden und von dieser `flowacct`-Instanz verwaltet werden. Der `usedmem`-Wert beträgt in diesem Beispiel 256. Der Wert für `usedmem` beträgt 0, wenn die Flow-Tabelle keine Flow-Datensätze enthält.

37

◆ ◆ ◆ KAPITEL 37

IPQoS im Detail (Referenz)

Dieses Kapitel enthält Referenzmaterialien mit ausführlichen Informationen zu den folgenden IPQoS-Themen:

- „IPQoS-Architektur und das Diffserv-Modell“ auf Seite 907
- „IPQoS-Konfigurationsdatei“ auf Seite 920
- „ipqosconf-Konfigurationsprogramm“ auf Seite 924

Eine Übersicht zu IPQoS finden Sie in Kapitel 32, „Einführung in IPQoS (Übersicht)“. Informationen zur Planung von IPQoS finden Sie in Kapitel 33, „Planen eines IPQoS-konformen Netzwerks (Aufgaben)“. Verfahren zur Konfiguration von IPQoS finden Sie in Kapitel 34, „Erstellen der IPQoS-Konfigurationsdatei (Aufgaben)“.

IPQoS-Architektur und das Diffserv-Modell

In diesem Abschnitt werden die IPQoS-Architektur und die Einflüsse von IPQoS auf das Differentiated Services (Diffserv)-Modell beschrieben, das unter RFC 2475, An Architecture for Differentiated Services (`http://www.ietf.org/rfc/rfc2475.txt?number=2475`) definiert ist. In IPQoS sind die folgenden Elemente des Diffserv-Modells enthalten:

- Classifier (Klassierer)
- Meter (Zähler)
- Marker (Zeiger)

Darüber hinaus umfasst IPQoS das Flow Accounting-Modul und den `dlcosmk`-Marker für die Verwendung mit Geräten für virtuelle lokale Netzwerke (VLANs).

Classifier-Modul

Im Diffserv-Modell ist ein *Classifier* für die Strukturierung der ausgewählten Verkehrswerte in Gruppen verantwortlich, an denen unterschiedliche Serviceebenen angewendet werden. Die in RFC 2475 definierten Classifier wurden ursprünglich für Grenzrouter konzipiert. Der

IPQoS-Classifier `ipgpc` dient jedoch zur Verarbeitung von Verkehrswerten auf Hosts, die sich in einem lokalen Netzwerk befinden. Somit kann ein Netzwerk mit IPQoS-Systemen und einem Diffserv-Router mehr Differentiated Services bereitstellen. Eine technische Beschreibung des `ipgpc`-Classifiers finden Sie in der Manpage `ipgpc`(7ipp).

Der `ipgpc`-Classifier führt Folgendes aus:

1. Wählt Verkehrswerte aus, der den in der IPQoS-Konfigurationsdatei auf dem IPQoS-konformen Systemen angegebenen Kriterien entsprechen

   Die QoS-Richtlinie definiert verschiedene Kriterien, die in den Paket-Headern vorhanden sein müssen. Diese Kriterien werden als *Selektoren* bezeichnet. Der `ipgpc`-Classifier vergleicht diese Selektoren mit den Paket-Headern, die vom IPQoS-System empfangen wurden. `ipgpc` wählt dann alle übereinstimmenden Pakete aus.
2. Teilt den Paketverkehr in *Klassen* (Netzverkehr mit den gleichen Eigenschaften) gemäß der Definition in der IPQoS-Konfigurationsdatei auf
3. Prüft den Wert im Differentiated Service (DS)-Feld des Pakets auf das Vorhandensein eines Differentiated Services Codepoint (DSCP)

   Das Vorhandensein des DSCP gibt an, ob der eingehende Verkehr vom Sender mit einem Weiterleitungsverhalten versehen wurde.
4. Ermittelt, welche weitere Aktion in der IPQoS-Konfigurationsdatei für die Pakete einer bestimmten Klasse definiert wurde
5. Übergibt die Pakete an das nächste in der IPQoS-Konfigurationsdatei angegebene IPQoS-Modul, gibt die Pakete an den Netzwerkdatenfluss zurück

Eine Übersicht zu diesem Classifier finden Sie unter „Classifier (`ipgpc`) – Übersicht“ auf Seite 831. Informationen zum Aufrufen des Classifiers in der IPQoS-Konfigurationsdatei finden Sie unter „IPQoS-Konfigurationsdatei“ auf Seite 920.

IPQoS-Selektoren

Der `ipgpc`-Classifier unterstützt verschiedene Selektoren, die Sie in der `filter`-Klausel der IPQoS-Konfigurationsdatei angeben können. Wenn Sie einen Filter definieren, verwenden Sie immer die Mindestanzahl an Selektoren, die zum erfolgreichen Abrufen von Datenverkehr für eine bestimmte Klasse erforderlich ist. Die Anzahl der von Ihnen definierten Filter kann sich auf die IPQoS-Performance auswirken.

In der folgenden Tabelle sind die für `ipgpc` verfügbaren Selektoren aufgeführt.

TABELLE 37–1 Filter-Selektoren für den IPQoS-Classifier

Selektor	Argument	Ausgewählte Informationen
`saddr`	IP-Adressnummer.	Quelladresse.
`daddr`	IP-Adressnummer.	Zieladresse.

TABELLE 37–1 Filter-Selektoren für den IPQoS-Classifier *(Fortsetzung)*

Selektor	Argument	Ausgewählte Informationen
`sport`	Entweder eine Portnummer oder ein Servicename gemäß der Definition in `/etc/services`.	Ursprungsport, von dem die Verkehrsklasse stammt.
`dport`	Entweder eine Portnummer oder ein Servicename gemäß der Definition in `/etc/services`.	Zielport, für den die Verkehrsklasse bestimmt ist.
`protocol`	Entweder eine Protokollnummer oder ein Protokollname gemäß der Definition in `/etc/protocols`.	Protokoll, das von dieser Verkehrsklasse verwendet werden muss.
`dsfield`	DS Codepoint (DSCP) mit einem Wert zwischen 0 und 63.	DSCP, der das Weiterleitungsverhalten für das Paket definiert. Wenn dieser Parameter angegeben ist, muss auch der Parameter `dsfield_mask` angegeben sein.
`dsfield_mask`	Bitmaske mit einem Wert zwischen 0 und 255.	Wird zusammen mit dem Selektor `dsfield` verwendet. `dsfield_mask` wird an dem Selektor `dsfield` angewendet, um festzustellen, welche Bit übereinstimmen müssen.
`if_name`	Schnittstellenname.	Schnittstelle, die entweder für eingehenden oder abgehenden Verkehr einer bestimmten Klasse verwendet werden muss.
`user`	Nummer der auszuwählenden UNIX-Benutzer-ID bzw. des auszuwählenden Benutzernamens. Wenn keine Benutzer-ID oder Benutzername im Paket vorhanden ist, wird der Standardwert –1 verwendet.	Die Benutzer-ID wird an eine Anwendung übermittelt.
`projid`	Nummer der auszuwählenden Projekt-ID.	Die Projekt-ID wird an eine Anwendung übermittelt.
`priority`	Prioritätsnummer. Die niedrigste Priorität ist 0.	Priorität, die Pakete dieser Klasse zugewiesen wird. Die Priorität dient zum Bestimmen der Wichtigkeit von Filtern für die gleiche Klasse.
`direction`	Argumente können eines der Folgenden sein:	Richtung des Paketflusses auf dem IPQoS-Computer.
	`LOCAL_IN`	Eingehender lokaler Verkehr zum IPQoS-System.
	`LOCAL_OUT`	Abgehender lokaler Verkehr zum IPQoS-System.
	`FWD_IN`	Eingehender, weiterzuleitender Verkehr.

TABELLE 37–1 Filter-Selektoren für den IPQoS-Classifier *(Fortsetzung)*

Selektor	Argument	Ausgewählte Informationen
	FWD_OUT	Abgehender, weiterzuleitender Verkehr.
precedence	Wert der Prioritätsstufe. Die höchste Prioritätsstufe ist 0.	Die Prioritätsstufe dient zum Sortieren von Filtern mit der gleichen Priorität.
ip_version	V4 oder V6	Von den Paketen verwendetes Adressierungsschema, entweder IPv4 oder IPv6.

Metermodul

Ein *Meter* verfolgt die Übertragungsrate von Datenströmen auf Paketbasis. Der Meter bestimmt, ob das Paket den konfigurierten Parametern entspricht. Das Metermodul bestimmt die nächste Aktion für ein Paket aus einer Reihe von Aktionen. Diese Aktion hängt von der Paketgröße, den konfigurierten Parametern und der Datenflussrate ab.

Der Meter besteht aus Metermodulen, `tokenmt` und `tswtclmt`, die Sie in der IPQoS-Konfigurationsdatei definieren. Sie können entweder ein Modul oder beide für eine Klasse konfigurieren.

Bei der Konfiguration eines Metermoduls können Sie zwei Parameter für die Rate definieren:

- `committed-rate` – Definiert die akzeptable Übertragungsrate in Bit pro Sekunde für Pakete einer bestimmten Klasse
- `peak-rate` – Definiert die maximale Übertragungsrate im Bit pro Sekunde, die für Pakete einer bestimmten Klasse zulässig ist

Eine Messaktion an einem Paket kann zu einem von drei möglichen Ergebnissen führen:

- `grün` – Das Paket führt dazu, dass der Datenfluss innerhalb der committed rate bleibt.
- `gelb` – Das Paket führt dazu, dass der Datenfluss die committed rate übersteigt, aber unter der peak rate bleibt.
- `rot` – Das Paket führt dazu, dass der Datenfluss die peak rate übersteigt.

Sie können jedes Ergebnis mit anderen Aktionen in der IPQoS-Konfigurationsdatei konfigurieren. Committed rate und peak rate werden im folgenden Abschnitt erklärt.

`tokenmt`-Metermodul

Das `tokenmt`-Modul verwendet *token buckets*, um die Übertragungsrate eines Datenflusses zu messen. Sie können `tokenmt` als Single-Rate- oder Two-Rate-Meter konfigurieren. Eine `tokenmt`-Aktionsinstanz verwaltet zwei Token Buckets, die feststellen, ob der Verkehrswert den konfigurierten Parametern entspricht.

Wie IPQoS das Token Meter-Paradigma umsetzt wird in der Manpage tokenmt(7ipp) beschrieben. Allgemeine Informationen zu Token Buckets finden Sie in Kalevi Kilkki's *Differentiated Services for the Internet* und auf verschiedenen anderen Websites.

Die Konfigurationsparameter für tokenmt sind:

- committed_rate – Legt die committed rate für den Datenfluss in Bit pro Sekunde fest.
- committed_burst – Legt die committed burst-Größe in Bit fest. Der committed_burst-Parameter legt fest, wie viele abgehende Pakete einer bestimmten Klasse bei committed rate in das Netzwerk passieren können.
- peak_rate – Legt die peak rate in Bit pro Sekunde fest.
- peak_burst – Legt die peak oder excess burst-Größe in Bit fest. Der peak_burst-Parameter gewährt einer Verkehrsklasse eine peak-burst-Größe, die die committed rate übersteigt.
- color_aware – Aktiviert den Erkennungsmodus für tokenmt.
- color_map – Definiert ein Array mit ganzen Zahlen, das DSCP-Werte den Farben grün, gelb und rot zuordnet.

Konfiguration von tokenmt als Single-Rate Meter

Um tokenmt als einen Single-Rate Meter zu konfigurieren, geben Sie keinen peak_rate-Parameter für tokenmt in der IPQoS-Konfigurationsdatei an. Damit eine Single-Rate tokenmt-Instanz das Ergebnis rot, grün oder gelb liefert, müssen Sie den peak_burst-Parameter angeben. Wenn Sie den peak_burst-Parameter nicht verwenden, kann tokenmt als Ergebnis nur rot oder grün liefern. Ein Beispiel für eine Single-Rate tokenmt mit zwei Ergebnissen finden Sie in Beispiel 34–3.

Wenn tokenmt als Single-Rate Meter eingesetzt wird, ist der peak_burst-Parameter tatsächlich die excess burst-Größe. committed_rate und entweder committed_burst oder peak_burst müssen positive ganze Zahlen ungleich Null sein.

Konfiguration von tokenmt als Two-Rate Meter

Um tokenmt als einen Two-Rate Meter zu konfigurieren, geben Sie einen peak_rate-Parameter für tokenmt in der IPQoS-Konfigurationsdatei an. Eine Two-Rate tokenmt-Instanz hat immer drei mögliche Ergebnisse: rot, gelb und grün. Die Parameter committed_rate, committed_burst und peak_burst müssen positive ganze Zahlen ungleich Null sein.

Konfiguration von tokenmt zur Erkennung von Farben

Damit eine Two-Rate tokenmt-Instanz Farben erkennen kann, müssen Sie zwei Parameter für die „Farberkennung„ spezifisch hinzufügen. Im Folgenden finden Sie ein Beispiel für eine action-Anweisung, die tokenmt zur Erkennung von Farben konfiguriert.

BEISPIEL 37–1 `tokenmt`-Aktion zur Farberkennung für die IPQoS-Konfigurationsdatei

```
action {
    module tokenmt
    name meter1
    params {
          committed_rate 4000000
          peak_rate 8000000
          committed_burst 4000000
          peak_burst 8000000
          global_stats true
          red_action_name continue
          yellow_action_name continue
          green_action_name continue
          color_aware true
          color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
    }
}
```

Sie aktivieren die Farberkennung, indem Sie den `color_aware`-Parameter auf `true` setzen. Als farbempfindliches Metermodul geht `tokenmt` davon aus, dass das Paket bereits in einer früheren `tokenmt`-Aktion mit rot, gelb oder grün markiert wurde. Ein farbbewusstes `tokenmt`-Modul wertet ein Paket aus, indem es den DSCP im Paket-Header zusätzlich zu den Parameter für ein Two-Rate Meter verwendet.

Der `color_map`-Parameter enthält ein Array, in dem der DSCP im Paket-Header zugeordnet ist. Betrachten Sie das folgende `color_map`-Array:

```
color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
```

Pakete mit einem DSCP zwischen 0 und 20 sowie 22 werden „grün" zugeordnet. Pakete mit einem DSCP von 21 und zwischen 23 und 42 sind „rot" zugeordnet. Pakete mit einem DSCP zwischen 43 und 63 sind„gelb" zugeordnet. `tokenmt` unterhält eine Standard-Farbkarte. Sie können die Standardeinstellungen jedoch Ihren Anforderungen entsprechend mit den `color_map`-Parameter anpassen.

In den *color*`_action_name`-Parameter können Sie `continue` angeben, um die Verarbeitung des Pakets abzuschließen. Oder Sie fügen ein Argument hinzu, um das Paket an eine Marker-Aktion zu senden, beispielsweise an `yellow_action_name` `mark22`.

`tswtclmt`-Metermodul

Das Metermodul `tswtclmt` schätzt die durchschnittliche Bandbreite einer Verkehrsklasse mithilfe eines Zeit-basierten *Rate Estimator*. `tswtclmt` wird immer als Three-Outcome Meter eingesetzt. Der Rate Estimator bietet eine Schätzung des eingehenden Datenverkehrs. Diese Rate muss etwa der laufenden durchschnittlichen Bandbreite des Datenflusses über eine bestimmte Zeit, dem *Zeitfenster* entsprechen. Der Rate Estimation-Algorithmus stammt aus RFC 2859, *A Time Sliding Window Three Colour Marker*.

Zur Konfiguration von `tswtclmt` verwenden Sie die folgenden Parameter:

- committed_rate – Legt die Committed Rate in Bit pro Sekunde fest
- peak_rate – Legt die Peak Rate in Bit pro Sekunde fest
- window – Definiert das Zeitfenster in Millisekunden, über das der Verlauf der durchschnittlichen Bandbreite erfasst wird

Technische Informationen zu tswtclmt finden Sie in der Manpage tswtclmt(7ipp) Allgemeine Information zu Rate Shapern, die ähnlich zu tswtclmt sind, finden Sie unter RFC 2963, A Rate Adaptive Shaper for Differentiated Services (http://www.ietf.org/rfc/rfc2963.txt?number=2963).

Markermodul

IPQoS umfasst die zwei Markermodule dscpmk und dlcosmk. In diesem Abschnitt wird beschrieben, wie Sie mit den beiden Markern arbeiten. Normalerweise verwenden Sie dscpmk, da dlcosmk nur für IPQoS-Systeme mit VLAN-Geräten zur Verfügung steht.

Technische Informationen zu dscpmk finden Sie in der Manpage dscpmk(7ipp). Technische Informationen zu dlcosmk finden Sie in der Manpage dlcosmk(7ipp).

Verwenden des Markers dscpmk zum Weiterleiten von Paketen

Der Marker empfängt Verkehrswerte, nachdem die Ströme von einem Classifier oder den Metermodulen verarbeitet wurden. Der Marker makiert den Datenverkehr mit einem Weiterleitungsverhalten. Dieses Weiterleitungsverhalten ist die Aktion, die an Datenströmen vorgenommen wird, nachdem die Datenströme das IPQoS-System verlassen haben. Das Weiterleitungsverhalten für eine Datenverkehrsklasse ist in dem *Per-Hop-Behavior (PHB)* festgelegt. Das PHB weist einer Datenverkehrsklasse eine bestimmte Priorität zu, die den Rang der Datenstöme einer Klasse gegenüber anderen Verkehrsklassen anzeigt. PHBs überwacht nur das Weiterleitungsverhalten in dem an das IPQoS-System angrenzenden Netzwerk. Weitere Informationen zu PHBs finden Sie unter „Per-Hop-Behaviors“ auf Seite 836.

Paketweiterleitung ist der Prozess des Sendens von Datenverkehr einer bestimmten Klasse an das nächste Ziel in einem Netzwerk. Bei einem Host wie einem IPQoS-System wird ein Paket vom Host an den lokalen Netzwerkdatenfluss weitergeleitet. Bei einem Diffserv-Router wird ein Paket von lokalen Netzwerk an den nächsten Hop des Routers weitergeleitet.

Der Marker markiert das DS-Feld im Paket-Header mit einem bekannten Weiterleitungsverhalten, das in der IPQoS-Konfigurationsdatei definiert ist. Danach leiten das IPQoS-System und nachfolgende Diffserv-konforme Systeme den Verkehr gemäß der Angabe im DS-Feld weiter, bis die Markierung geändert wird. Um ein PHB zuzuweisen, markiert das IPQoS-System einen Wert im DS-Feld des Paket-Headers. Dieser Wert wird als der Differentiated Services Codepoint (DSCP) bezeichnet. Die Diffserv-Architektur definiert zwei Arten von Weiterleitungsverhalten, EF und AF, die unterschiedliche DSCPs verwenden. Eine Einführung in DSCPs finden Sie unter „DS Codepoint“ auf Seite 836.

Das IPQoS-System liest den DSCP für den Verkehrswert ein und wertet die Prioritätsstufe des Datenflusses in Relation zu anderen abgehenden Verkehrswerten aus. Dann priorisiert das IPQoS-System alle gleichzeitig auftretenden Verkehrswerte und gibt jeden Strom nach seiner Priorität in das Netzwerk frei.

Der Diffserv-Router empfängt abgehende Verkehrswerte und liest das DS-Feld in den Paket-Headern ein. Anhand des DSCP kann der Router gleichzeitig auftretende Verkehrswerte priorisieren und planen. Dann leitet der Router jeden Datenfluss nach der Priorität weiter, die durch das PHB angegeben ist. Beachten Sie, dass das PHB nicht über den Grenzrouter des Netzwerk hinaus Anwendung findet, es sei denn, Diffserv-konforme Systeme in den nachfolgenden Hops erkennen das gleiche PHB.

Expedited Forwarding (EF) PHB

Expedited forwarding (EF) garantiert, dass Pakete mit dem empfohlenen EF Codepoint 46 (101110) die beste Behandlung erfahren, die zur Freigabe in das Netzwerk verfügbar ist. Expedited Forwarding wird häufig mit einer Standleitung verglichen. Pakete mit dem Codepoint 46 (101110) erhalten eine garantierte bevorzugte Behandlung von allen Diffserv-Routern auf dem Weg zum Ziel der Pakete. Technische Informationen zum EF finden Sie in der RFC 2598, *An Expedited Forwarding PHB*.

Assured Forwarding (AF) PHB

Assured Forwarding (AF) bietet vier verschiedene Klassen für das Weiterleitungsverhalten, das Sie für den Marker angeben können. Die folgende Tabelle zeigt die Klassen, die drei drop-Prioritätsstufen, die mit jeder Klasse bereitgestellt werden, und die empfohlenen DSCPs, die jeder Prioritätsstufe zugeordnet sind. Jeder DSCP wird durch seinen AF-Wert, seinem dezimalen Wert und seinem binären Wert dargestellt.

TABELLE 37–2 Assured Forwarding Codepoints

	Klasse 1	Klasse 2	Klasse 3	Klasse 4
Low-Drop-Prioritätsstufe	AF11 = 10 (001010)	AF21 = 18 (010010)	AF31 = 26 (011010)	AF41 = 34 (100010)
Medium-Drop-Prioritätsstufe	AF12 = 12 (001100)	AF22 = 20 (010100)	AF32 = 28 (011100)	AF42 = 36 (100100)
High-Drop-Prioritätsstufe	AF13 = 14 (001110)	AF23 = 22 (010110)	AF33 = 30 (011110)	AF43 = 38 (100110)

Jedes Diffserv-konforme System kann den AF Codepoint als Leitfaden zum Bereitstellen von differenzierten Weiterleitungsverhalten für verschiedene Verkehrsklassen verwenden.

Wenn diese Pakete einen Diffserv-Router erreichen, wertet der Router die Codepoints der Pakete zusammen mit den DSCPs anderen Datenverkehrs in der Warteschlange aus. Abhängig von der verfügbaren Bandbreite und den Prioritäten gemäß den Paket-DSCPs leitet der Router die Pakete dann entweder weiter oder wirft sie ab. Pakete, die mit dem EF PHB gekennzeichnet sind, erhalten eine garantierte Bandbreite im Vergleich zu Paketen, die mit den verschiedenen anderen AF PHBs gekennzeichnet sind.

Koordinieren Sie die Paketmarkierung zwischen den IPQoS-Systemen in Ihrem Netzwerk und dem Diffserv-Router, um sicherzustellen, dass die Pakete wie erwartet weitergeleitet werden. Angenommen, die IPQoS-Systeme in Ihrem Netzwerk markieren die Pakete mit den Codepoints AF21 (010010), AF13 (001110), AF43 (100110) und EF (101110). In diesem Fall müssen Sie die DSCPs AF21, AF13, AF43 und EF zur entsprechenden Datei auf dem Diffserv-Router hinzufügen.

Eine technische Erläuterung der AF-Codepoint-Tabelle finden Sie in der Norm RFC 2597. Die Router-Hersteller Cisco Systems und Juniper Networks veröffentlichen ausführliche Information zur AF PHB-Einstellung auf ihren Websites. Sie können diese Informationen sowohl zum Definieren von AF PHBs für IPQoS-Systeme als auch für Router verwenden. Darüber hinaus enthält die Dokumentation der Router-Hersteller Anweisungen zum Einrichten der DS Codepoints auf ihren Geräten.

Bereitstellen eines DSCP für einen Marker

Der DSCP ist 6 Bit lang. Das DS-Feld ist 1 Byte lang. Wenn Sie einen DSCP definieren, markiert der Marker die ersten sechs Bit des Paket-Headers mit dem DS Codepoint. Die verbleibenden zwei Bit bleiben unbenutzt.

Zum Definieren eines DSCP verwenden Sie den folgenden Parameter innerhalb einer Marker action-Anweisung:

```
dscp_map{0-63:DS_codepoint}
```

Der `dscp_map`-Parameter ist ein Array mit 64 Elementen, das Sie mit dem (DSCP)-Wert füllen. `dscp_map` wird zum Zuordnen von eingehenden DSCPs zu abgehenden DSCPs verwendet, die vom `dscpmk`-Marker angewendet werden.

Sie müssen den DSCP-Wert für `dscp_map` im Dezimalformat angeben. Beispielsweise müssen Sie den EF Codepoint 101110 in den Dezimalwert 46 übertragen: `dscp_map{0-63:46}`. Bei AF Codepoints müssen Sie die verschiedenen Codepoints aus Tabelle 37–2 für die Verwendung durch `dscp_map` in die dezimale Notation übertragen.

Verwenden des Markers `dlcosmk` mit VLAN-Geräten

Das Markermodul `dlcosmk` markiert ein Weiterleitungsverhalten im MAC-Header eines Datagramms. `dlcosmk` können Sie nur in einem IPQoS-System mit einer VLAN-Schnittstelle einsetzen.

`dlcosmk` fügt dem VLAN-Header vier Byte hinzu, die als *VLAN-Tag* bezeichnet werden. Das VLAN-Tag enthält einen 3-Bit-Wert für die Benutzerpriorität, der vom IEEE 801.D-Standard definiert wird. Diffserv-konforme Switches, die VLAN verstehen, können ein Benutzerpriorität-Feld in einem Datagramm lesen. Die 801.D-Benutzerprioritätswerte implementieren die Serviceklassen (CoS)-Markierungen, die kommerziellen Switches bekannt sind und von ihnen verstanden werden.

Sie verwenden die Benutzerprioritätswerte in der `dlcosmk`-Markeraktion, indem Sie die in der folgenden Tabelle aufgeführten Serviceklassenmarkierungen definieren.

TABELLE 37–3 801.D-Benutzerprioritätswerte

Serviceklasse	Definition
0	Beste Leistung
1	Hintergrund
2	Spare
3	Exzellente Leistung
4	Kontrollierte Last
5	Video weniger als 100 ms Latenz
6	Video weniger als 10 ms Latenz
7	Netzwerkkontrolle

Weitere Informationen zu `dlcosmk` finden Sie in der Manpage `dlcosmk`(7ipp).

IPQoS-Konfiguration für Systeme mit VLAN-Geräten

In diesem Abschnitt wird ein einfaches Netzwerkszenario vorgestellt, mit dem gezeigt wird, wie IPQoS auf Systemen mit VLAN-Geräten implementiert wird. Das Szenario umfasst zwei IPQoS-Systeme, `machine1` und `machine2`, die über einen Switch miteinander verbunden sind. Das VLAN-Gerät in `machine1` hat die IP-Adresse `10.10.8.1`. Das VLAN-Gerät in `machine2` hat die IP-Adresse `10.10.8.3`.

Die folgende IPQoS-Konfigurationsdatei für `machine1` zeigt eine einfache Lösung zum Markieren von Datenverkehr über den Switch an `machine2`.

BEISPIEL 37–2 IPQoS-Konfigurationsdatei für ein System mit einem VLAN-Gerät

```
fmt_version 1.0
action {
        module ipgpc
          name ipgpc.classify

        filter {
```

BEISPIEL 37–2 IPQoS-Konfigurationsdatei für ein System mit einem VLAN-Gerät *(Fortsetzung)*

```
                name myfilter2
                daddr 10.10.8.3
                class myclass
        }

        class {
                name myclass
                next_action mark4
        }
}

action {
        name mark4
        module dlcosmk
        params {
                cos 4
                next_action continue
        global_stats true
        }
}
```

Bei dieser Konfiguration wird jeglicher Datenverkehr von `machine1`, der für das VLAN-Gerät in `machine2` bestimmt ist, an den `dlcosmk`-Marker übergeben. Die Markeraktion `mark4` weist `dlcosmk` an, Datagrammen der Klasse `myclass` mit einem CoS von 4 ein VLAN-Mark zuzuweisen. Der Benutzerprioritätswert 4 gibt an, dass der Switch zwischen beiden Rechnern Traffic-Flows vom Typ `myclass` kontrollierte Lastenweiterleitung von `machine1` zuweisen soll.

`flowacct`-Modul

Das IPQoS `flowacct`-Modul zeichnet Informationen zu den Verkehrswerten auf, ein Vorgang, der als *Flow Accounting* bezeichnet wird. Das Flow Accounting erzeugt Daten, die entweder zur Rechnungsstellung für Kunden oder zur Auswertung der Menge an Datenverkehr einer bestimmten Klasse verwendet werden können.

Das Flow Accounting ist optional. `flowacct` ist in der Regel das letzte Modul, auf das ein gemessener oder markierter Verkehrswert trifft, bevor er in den Netzwerkstrom freigegeben wird. Eine Darstellung der Position von `flowacct` im Diffserv-Modell finden Sie in Abbildung 32–1. Ausführliche technische Informationen zu `flowacct` finden Sie in der Manpage `flowacct`(7ipp).

Zum Aktivieren des Flow Accounting benötigen Sie die Oracle Solaris Accounting-Funktion `exacct` und den Befehl `acctadm` sowie `flowacct`. Allgemeine Schritte zum Einrichten des Flow Accounting finden Sie unter „Einrichten des Flow Accounting (Übersicht der Schritte)“ auf Seite 901.

`flowacct`-Parameter

Das `flowacct`-Modul sammelt Informationen zu den Datenströmen in einer *Flow-Tabelle* mit *Flow-Datensätzen*. Jeder Eintrag in der Tabelle enthält einen Flow-Datensatz. Sie können eine Flow-Tabelle nicht anzeigen.

In der IPQoS-Konfigurationsdatei definieren Sie die folgenden `flowacct`-Parameter, um die Flow-Datensätze zu messen und in die Flow-Tabelle zu schreiben:

- `timer` – Definiert ein Zeitintervall in Millisekunden, nach dem Datenströmen mit einer Zeitüberschreitung aus der Flow-Tabelle entfernt und in eine Datei geschrieben werden, die von `acctadm` erstellt wird.
- `timeout` – Definiert ein Zeitintervall in Millisekunden, mit dem festgelegt wird, wie lange ein Paketdatenfluss inaktiv sein muss bis eine Zeitüberschreitung eintritt

---

Hinweis – Sie können `timer` und `timeout` mit unterschiedlichen Werten konfigurieren.

- `max_limit` – Legt einen oberen Grenzwert für die Anzahl an Flow-Datensätze fest, die in der Flow-Tabelle gespeichert werden können

Ein Beispiel für die Anwendung von `flowacct`-Parameter in der IPQoS-Konfigurationsdatei finden Sie unter „So konfigurieren Sie die Verkehrssteuerung in der IPQoS-Konfigurationsdatei“ auf Seite 887.

Flow-Tabelle

Das `flowacct`-Modul verwaltet eine Flow-Tabelle, in der alle Paket-Datenströme aufgezeichnet werden, die von einer `flowacct`-Instanz erfasst werden. Ein Datenfluss wird durch die folgenden Parameter gekennzeichnet, die in dem `flowacct` 8–Tuple enthalten sind:

- Quelladresse
- Zieladresse
- Ursprungs-Port
- Ziel-Port
- DSCP
- Benutzer-ID
- Projekt-ID
- Protokollnummer

Wenn alle Parameter des 8–Tuple für einen Datenfluss gleich bleiben, enthält die Flow-Tabelle nur einen einzigen Eintrag. Der `max_limit`-Parameter legt die Anzahl an Einträgen fest, die eine Flow-Tabelle aufnehmen kann.

Die Flow-Tabelle wird in dem Intervall gescannt, das für den `timer`-Parameter in der IPQoS-Konfigurationsdatei angegeben ist. Die Standardeinstellung beträgt 15 Sekunden. Ein Datenfluss erfährt einen „Timeout“, wenn das IPQoS-System mindestens über das in der

IPQoS-Konfigurationsdatei festgelegte `timeout`-Intervall keine Pakete dieses Datenflusses erfasst. Das standardmäßige Timeout-Intervall beträgt 60 Sekunden. Einträge, für die ein Timeout eingetreten ist, werden in die zuvor mit dem Befehl `acctadm` erstellte Accounting-Datei geschrieben.

`flowacct`-Datensätze

Ein `flowacct`-Datensatz enthält die in der folgenden Tabelle beschriebenen Attribute.

TABELLE 37–4 Attribute eines `flowacct`-Datensatzes

Attributname	Attributinhalt	Typ
`src-addr-`*Adresstyp*	Ursprungsadresse des Absenders. *Adresstyp* ist entweder `v4` für IPv4 oder `v6` für IPv6, je nach Angabe in der IPQoS-Konfigurationsdatei.	Basic
`dest-addr-`*Adresstyp*	Zieladresse der Pakete. *Adresstyp* ist entweder `v4` für IPv4 oder `v6` für IPv6, je nach Angabe in der IPQoS-Konfigurationsdatei.	Basic
`src-port`	Ursprungs-Port, von dem Verkehrsfluss stammt.	Basic
`dest-port`	Ziel-Port, für den dieser Verkehrsfluss bestimmt ist.	Basic
`protocol`	Protokollnummern des Verkehrsflusses.	Basic
`total-packets`	Anzahl der Pakete im Verkehrsfluss.	Basic
`total-bytes`	Anzahl der Byte im Verkehrsfluss.	Basic
Aktionsname	Name der `flowacct`-Aktion, die diesen Verkehrsfluss aufgezeichnet hat.	Basic
`creation-time`	Uhrzeit, wann das erste Paket des Verkehrsflusses von `flowacct` erfasst wurde.	Nur Extended
`last-seen`	Uhrzeit, wann zuletzt ein Paket des Verkehrsflusses erfasst wurde.	Nur Extended
`diffserv-field`	DSCP in den Headern abgehender Pakete im Verkehrsfluss.	Nur Extended
`user`	Entweder eine UNIX-Benutzer-ID oder ein Benutzername, der von der Anwendung bezogen wird.	Nur Extended
`projid`	Projekt-ID, die von der Anwendung bezogen wird.	Nur Extended

Verwenden von `acctadm` mit dem `flowacct`-Modul

Mit dem Befehl `acctadm` können Sie eine Datei erstellen, in der die verschiedenen vom `flowacct`-Modul erzeugten Flow-Datensätze gespeichert werden. `acctadm` arbeitet mit der Extended Accounting-Funktion zusammen. Technische Informationen zu `acctadm` finden Sie in der Manpage `acctadm`(1M).

Das `flowacct`-Modul überwacht Verkehrsflüsse und füllt die Flow-Tabelle mit Flow-Datensätzen. Dann wertet `flowacct` seine Parameter und Attribute in dem von `timer` vorgegebenen Intervall aus. Wenn ein Paket über die Werte `last_seen` plus `timeout` nicht erfasst wird, tritt ein Timeout für das Paket auf. Alle Einträge mit einem Timeout werden aus der Flow-Tabelle gelöscht. Diese Einträge werden dann in dem durch den Parameter `timer` vorgegebenen Intervall in die Accounting-Datei geschrieben.

Zum Aufrufen von `acctadm` für das `flowacct`-Modul verwenden Sie die folgende Befehlssyntax:

`acctadm -e` *file-type* `-f` *filename* `flow`

`acctadm -e` — Ruft `acctadm` mit der Option `-e` auf. Das -e gibt an, dass eine Ressourcenliste folgt.

Dateityp — Gibt die zu erfassenden Attribute an. *Dateityp* muss durch entweder `basic` oder `extended` ersetzt werden. Eine Liste der Attribute für jeden Dateityp finden Sie in Tabelle 37–4.

`-f`*Dateiname* — Erstellt die Datei *Dateiname*, in der die Flow-Datensätze gespeichert werden.

`flow` — Gibt an, dass `acctadm` mit IPQoS ausgeführt wird.

IPQoS-Konfigurationsdatei

In diesem Abschnitt finden Sie Informationen zu den einzelnen Teilen der IPQoS-Konfigurationsdatei. Die beim Booten aktivierte IPQoS-Richtlinie ist in der Datei `/etc/inet/ipqosinit.conf` gespeichert. Obwohl Sie diese Datei bearbeiten können, sollten Sie für ein neues IPQoS-System eine Konfigurationsdatei mit einem anderen Namen erstellen. Aufgaben zum Übernehmen und Debuggen einer IPQoS-Konfiguration finden Sie in Kapitel 34, „Erstellen der IPQoS-Konfigurationsdatei (Aufgaben)“.

Die Syntax der IPQoS-Konfigurationsdatei ist in Beispiel 37–3 gezeigt. Das Beispiel verwendet die folgenden typografischen Konventionen:

- `Computerstil-Typ` – Syntaktische Informationen, mit denen Teile der Konfigurationsdatei beschrieben werden. Sie geben keinen Text ein, der im Computerstil-Typ angezeigt wird.
- **`Fettdruck`** – Literaltext, den Sie in die IPQoS-Konfigurationsdatei eingeben müssen. Beispielsweise müssen Sie die IPQoS-Konfigurationsdatei stets mit **`fmt_version`** beginnen.

- *Kursivdruck* – Variablentext, den Sie durch beschreibende Informationen zu Ihrer Konfiguration ersetzen. Beispielsweise müssen Sie stets *action-name* oder *module-name* durch Informationen ersetzen, die für Ihre Konfiguration gelten.

BEISPIEL 37–3 Syntax der IPQoS-Konfigurationsdatei

```
file_format_version ::= fmt_version version

action_clause ::= action {
     name action-name
     module module-name
     params-clause |  ""
     cf-clauses
}
action_name ::= string
module_name ::= ipgpc | dlcosmk | dscpmk | tswtclmt | tokenmt | flowacct

params_clause ::= params {
     parameters
     params-stats |   ""
     }
parameters ::=     prm-name-value parameters |  ""
prm_name_value ::= param-name param-value

params_stats ::= global-stats boolean

cf_clauses ::= class-clause cf-clauses |
               filter-clause cf-clauses | ""

class_clause ::= class {
     name class-name
     next_action next-action-name
     class-stats | ""
                 }
class_name  ::= string
next_action_name  ::= string
class_stats ::= enable_stats boolean
boolean ::= TRUE | FALSE

filter_clause ::= filter {
                name filter-name
                class class–name
                parameters
                }
filter_name ::= string
```

Im Folgenden werden die wichtigsten Teile der IPQoS-Konfigurationsdatei beschrieben.

`action`-Anweisung

Mit `action`-Anweisungen rufen Sie die verschiedenen IPQoS-Module auf, die unter „IPQoS-Architektur und das Diffserv-Modell“ auf Seite 907 beschrieben sind.

Achten Sie darauf, dass eine IPQoS-Konfigurationsdatei immer mit der Versionsnummer beginnen muss. Dann müssen Sie die folgende `action`-Anweisung hinzufügen, um den Classifier aufzurufen:

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
}
```

Nach der Classifier `action`-Anweisung geben Sie eine `params`-Klausel oder eine `class`-Klausel ein.

Verwenden Sie für alle `action`-Anweisungen die folgende Syntax:

```
action {
name action-name
module module-name
params-clause | ""
cf-clauses
}
```

`name` *action_name* — Weist der Aktion einen Namen zu.

`module` *module_name* — Identifiziert das aufzurufende IPQoS, bei dem es sich um eines der Module in Tabelle 37–5 handeln muss.

params_clause — Können Parameter für den zu verarbeitenden Classifier sein, z. B. globale Statistiken oder die nächste zu verarbeitende Aktion.

cf_clauses — Eine Reihe von null oder mehr `class`- oder `filter`-Klauseln

Definition der Module

Die Moduldefinition gibt an, welches Modul in den Parametern der `action`-Anweisung verarbeitet werden soll. Die IPQoS-Konfigurationsdatei kann die folgenden Module enthalten.

TABELLE 37–5 IPQoS-Module

Modulname	Definition
`ipgpc`	IP-Classifier
`dscpmk`	Zum Erstellen von DSCPs in IP-Paketen zu verwendender Marker

TABELLE 37–5 IPQoS-Module (Fortsetzung)

Modulname	Definition
dlcosmk	Mit VLAN-Geräten zu verwendender Marker
tokenmt	Token Bucket-Metermodul
tswtclmt	Time-Sliding Window-Metermodul
flowacct	Flow Accounting-Modul

class-Klausel

Sie definieren eine class-Klausel für jede Verkehrsklasse.

Zum Definieren der verbleibenden Klassen in der IPQoS-Konfiguration verwenden Sie die folgende Syntax:

```
class {

       name class-name
       next_action next-action-name
}
```

Um die Erfassung von Statistiken einer bestimmten Klasse zu aktivieren, müssen Sie zunächst die globalen Statistiken in der ipgpc.classify action-Anweisung aktivieren. Weitere Informationen hierzu finden Sie unter „action-Anweisung“ auf Seite 921.

Mit der enable_stats TRUE-Anweisung können Sie Erfassung von Statistiken für eine Klasse jederzeit aktivieren. Wenn Sie keine Statistiken für eine Klasse erfassen möchten, können Sie die enable_stats FALSE-Anweisung verwenden. Alternativ löschen Sie die enable_stats-Anweisung.

Verkehr in einem IPQoS-konformen Netzwerk, den Sie nicht speziell definieren, wird der *Standardklasse* zugeordnet.

filter-Klausel

Filter bestehen aus Selektoren, die Verkehrswerte in Klassen gruppieren. Diese Selektoren definieren die Kriterien, die an dem Verkehr einer in der class-Klausel erstellten Klasse angewendet werden. Wenn ein Paket allen Selektoren des Filters mit der höchsten Priorität entspricht, wird es als ein Mitglied dieser Filterklasse betrachtet. Eine vollständige Liste der Selektoren, die Sie mit dem ipgpc-Classifier verwenden können, finden Sie unter Tabelle 37–1.

Die Filter in der IPQoS-Konfigurationsdatei werden mithilfe einer *filter*-Klausel definiert, die folgende Syntax aufweist:

```
filter {
       name filter-name
       class class-name
       parameters (selectors)
       }
```

params-Klausel

Die params-Klausel enthält Verarbeitungsanweisungen für das in der action-Anweisung definierte Modul. Für die params-Klausel verwenden Sie die folgende Syntax:

```
params {
           parameters
           params-stats | ""
       }
```

In der params-Klausel verwenden Sie Parameter, die an dem Modul angewendet werden können.

Der Wert *params-Statistiken* in der params muss entweder global_stats TRUE oder global_stats FALSE lauten. Die Anweisung global_stats TRUE aktiviert die Erfassung von Statistiken im UNIX-Stil für die action-Anweisung, in der die globalen Statistiken aufgerufen werden. Statistiken können Sie mithilfe des Befehls kstat anzeigen. Sie müssen die action-Anweisung aktivieren, bevor Sie die Erfassung von Statistiken pro Klasse aktivieren können.

ipqosconf-Konfigurationsprogramm

Mit dem Serviceprogramm ipqosconf können Sie die IPQoS-Konfigurationsdatei einlesen und die IPQoS-Module im UNIX-Kernel konfigurieren. ipqosconf führt die folgenden Aktionen aus:

- Übernimmt die Konfigurationsdatei für die IPQoS-Kernelmodule (ipqosconf -a *Dateiname*)
- Listet die IPQoS-Konfigurationsdatei auf, die derzeit im Kernel enthalten ist (ipqosconf -l)
- Stellt sicher, dass die aktuelle IPQoS-Konfiguration eingelesen und bei jedem Neustart des Computers angewendet wird (ipqosconf -c)
- Leert die aktuellen IPQoS-Kernelmodule (ipqosconf -f)

Technische Informationen finden Sie in der Manpage ipqosconf(1M).

Glossar

Dieses Glossar enthält Definitionen der neu in diesem Handbuch eingeführten Begriffe, die nicht im *Glossar* auf der Website `docs.sun.com` aufgeführt sind.

3DES
Lesen Sie dazu Triple-DES.

Adressmigration
Die Adressmigration ist ein Prozess, bei dem eine Adresse von einer Netzwerkschnittstelle zu einer anderen Netzwerkschnittstelle verschoben wird. Die Adressmigration ist ein Teil des Failover-Prozesses (wenn eine Schnittstelle ausfällt), oder des Failback-Prozesses (wenn eine Schnittstelle repariert wurde).

Adresspool
Unter Mobile IP ein Adressensatz, der vom Home-Netzwerk-Administrator für die Verwendung durch mobile Knoten zugewiesen werden, die eine Home-Adresse benötigen.

AES
Advanced Encryption Standard. Eine symmetrische 128-Bit Blockdaten-Verschlüsselungstechnik. Die U.S.-Regierung hat die Rijndael-Variante des Algorithmus im Oktober 2000 als Verschlüsselungsstandard angenommen. AES ersetzt die DES-Verschlüsselung als Regierungsstandard.

Agent Advertisement-Nachricht
Unter Mobile IP eine Nachricht, die in regelmäßigen Abständen von Home-Agents und Foreign-Agents gesendet wird, um deren Vorhandensein auf den angeschlossenen Links bekannt zu geben.

Agent-Erkennung
Unter Mobile IP der Prozess, mit dem ein mobiler Knoten feststellt, ob er verschoben wurde, seinen aktuellen Standort erkennt und die Adresse im Foreign-Netzwerk ermittelt.

Anycast-Adresse
Eine IPv6-Adresse, die einer Schnittstellengruppe zugewiesen wurde (die in der Regel zu unterschiedlichen Knoten gehören). Ein an eine Anycast-Adresse gerichtetes Paket wird an die *nächste* Schnittstelle mit dieser Adresse geleitet. Die Paketroute entspricht der mit dem Routing-Protokoll gemessenen Strecke.

Anycast-Gruppe
Eine Schnittstellengruppe mit der gleichen Anycast-IPv6-Adresse. Das Erstellen von Anycast-Adressen und -Gruppen wird in Oracle Solaris nicht unterstützt. Jedoch können Oracle Solaris IPv6-Knoten Verkehr an Anycast-Gruppen senden.

Asymmetric Key Cryptography Ein Verschlüsselungssystem, bei dem Sender und Empfänger einer Nachricht unterschiedliche Schlüssel zum Verschlüsseln und Entschlüsseln der Nachricht verwenden. Asymmetrische Schlüssel werden verwendet, um einen sicheren Kanal für die Verschlüsselung mit symmetrischen Schlüsseln aufzubauen. Das Diffie-Hellman-Protokoll ist ein Beispiel für eine Protokoll mit asymmetrischen Schlüsseln. Vergleichen Sie mit Symmetrische Schlüssel-Kryptographie.

Ausfallerkennung Das Erkennen, dass eine Schnittstelle oder ein Pfad von einer Schnittstelle zu einem Gerät auf der Internetschicht nicht mehr funktioniert. IP Network Multipathing (IPMP) umfasst zwei Arten der Ausfallerkennung: Link-basiert (die Standardeinstellung) und Stichproben-basiert (optional).

Authentication Header Ein Erweiterungsheader, der IP-Datagrammen Authentifizierung und Integrität, allerdings keine Vertraulichkeit bietet.

Autokonfiguration Der Prozess, bei dem ein Host seine IPv6-Adresse automatisch aus dem Standortpräfix und der lokalen MAC-Adresse konfiguriert.

Benutzerpriorität Ein 3-Bit-Wert, der Serviceklassen-Markierungen implementiert, die definieren, wie Ethernet-Datagramme in einem Netzwerk mit VLAN-Geräten weitergeleitet werden.

Bidirektionaler Tunnel Ein Tunnel, der Datagramme in beide Richtungen übertragen kann.

Bindungstabelle Unter Mobile IP eine Home-Agent-Tabelle, die eine Home-Adresse zu einer Care-Of-Adresse zuordnet, einschließlich verbleibender Lebensdauer und gewährte Zeit.

Blowfish Ein symmetrischer Blockzifferalgorithmus, der einen Schlüssel mit variabler Länge zwischen 32 und 448 Bit akzeptiert. Der Autor, Bruce Schneier, ist der Meinung, dass Blowfish für Anwendungen optimiert ist, bei denen der Schlüssel nicht häufig geändert wird.

Broadcast-Adresse IPv4-Netzwerkadressen, bei denen die Host-Komponente der Adresse entweder ausschließlich Nullen (10.50.0.0) oder nur Einerbits (10.50.255.255) aufweist. Ein von einem Computer in lokalen Netz an eine Broadcast-Adresse gesendetes Paket wird allen Computern in diesem Netzwerk zugestellt.

CA Siehe Zertifizierungsstelle (Certificate authority, CA).

Care-Of-Adresse Eine vorübergehende Adresse eines mobilen Knotens, die als Tunnelendpunkt verwendet wird, wenn der mobile Knoten an ein Foreign-Netzwerk angeschlossen ist.

Classless Inter-Domain Routing (CIDR)-Adresse Eine Adresse im IPv4-Format, die nicht auf den Netzwerkklassen basiert (Klasse A, B und C). CIDR-Adressen weisen eine Länge von 32 Bit auf. Sie verwenden die standardmäßige getrennte dezimale IPv4-Format zuzüglich eines Netzwerkpräfix. Dieses Präfix definiert die Netzwerknummer und die Netzwerkmaske.

Datagramm Siehe IP-Datagramm.

Datenadresse — Die IP-Adresse, die als Quell- oder Zieladresse für Daten verwendet werden kann. Datenadressen sind Teil einer IPMP-Gruppe und können zum Senden und Empfangen von Datenverkehr an einer beliebigen Schnittstelle in der Gruppe verwendet werden. Darüber hinaus kann der Datenadressensatz in einer IPMP-Gruppe ständig verwendet werden, vorausgesetzt, eine Schnittstelle der Gruppe arbeitet ordnungsgemäß.

`DEPRECATED` **(eingestellte) Adresse** — Eine IP-Adresse, die nicht als Quell- oder Zieladresse für Daten in einer IPMP-Gruppe verwendet werden kann. In der Regel sind IPMP-Testadressen `DEPRECATED` . Es kann jedoch jede Adresse als `DEPRECATED` gekennzeichnet werden, um zu verhindern, dass diese Adresse als Quelladresse verwendet wird.

DES — Data Encryption Standard. Eine 1975 entwickelte und 1981 als ANSI X.92.56 von ANSI standardisierte symmetrische Verschlüsselungsmethode. DES verwendet einen 56-Bit-Schlüssel.

Diffie-Hellman-Protokoll — Wird auch als PublicKey-Kryptographie bezeichnet. Ein von Diffie und Hellman 1976 entwickeltes asymmetrisches Kryptographieprotokoll zum Schlüsselaustausch. Mithilfe dieses Protokolls können zwei Benutzer einen Geheimschlüssel über einen nicht datensicheren Übertragungskanal austauschen. Diffie-Hellman wird vom IKE-Protokoll verwendet.

Diffserv-Modell — Internet Engineering Task Force Architekturstandard zur Umsetzung von Differentiated Services in IP-Netzwerken. Die wichtigsten Module sind Classifier, Meter, Marker, Scheduler und Dropper. IPQoS implementiet die Module Classifier, Meter und Marker. Das Diffserv-Modell ist in RFC 2475, *An Architecture for Differentiated Services* beschrieben.

Digitale Signatur — Ein digitaler Code, der an eine elektronisch übermittelte Nachricht angehängt ist und die den Absender eindeutig identifiziert.

Domain of Interpretation (DOI) — Eine DOI definiert Datenformate, Netzverkehr-Austauscharten sowie Konventionen für das Benennen von sicherheitsrelevanten Informationen. Bespiele für sicherheitsrelevante Informationen sind Sicherheitsrichtlinien, kryptografische Algorithmen und Kryptographiemodi.

DS Codepoint (DSCP) — Ein 6-Bit-Wert, der angibt, wie ein Paket weitergeleitet werden muss, wenn er in das DS-Feld eines IP-Header aufgenommen ist.

DSA — Digital Signature Algorithm. Ein PublicKey-Algorithmus mit einer variablen Schlüsselgröße zwischen 512 und 4096 Bit. Das Standard der US-Regierung, DSS, verwendet bis zu 1024 Bit. DSA verlässt sich zur Eingabe auf SHA-1.

Dual Stack — Ein TCP/IP-Protokollstapel mit IPv4 und IPv6 in der Netzwerkschicht. Die verbleibenden Stapel sind identisch. Wenn Sie IPv6 während der Installation von Oracle Solaris aktivieren, empfängt der Host die Dual Stack-Version von TCP/IP.

Dynamic Reconfiguration (DR) — Ist die Fähigkeit, ein System im laufenden Zustand ohne oder mit nur geringen Auswirkungen auf vorhandene Vorgänge neu zu konfigurieren. Nicht alle Sun-Plattformen unterstützen DR. Einige Sun-Plattformen unterstützen DR nur bei bestimmten Hardwaretypen (z. B. NICs).

Dynamischer Paketfilter — Siehe Statusbehafteter Paketfilter.

Encapsulating Security Payload (ESP) Ein Erweiterungsheader, der Datagrammen Integrität und Vertraulichkeit bietet. ESP ist eine der fünf Komponenten der IP Security Architecture (IPsec).

Ergebnis Die Aktion, die als Resultat des gemessenen Verkehrs durchgeführt wird. Die IPQoS-Meter haben drei Ergebnisse: rot, gelb und grün, die in der IPQoS-Konfigurationsdatei definiert werden.

Failback Der Netzwerkzugriff wird auf eine Schnittstelle zurückgeschaltet, deren Reparatur erkannt wurde.

Failover Der Netzwerkzugriff wird von einer ausgefallenen Schnittstelle auf eine ordnungsgemäß arbeitende physikalische Schnittstelle umgeschaltet. Netzwerkzugriff umfasst IPv4 Unicast-, Multicast- und Broadcast-Verkehr sowie IPv6 Unicast- und Multicast-Verkehr.

Filter Eine Liste mit Regeln, die die Eigenschaften einer Klasse in der IPQoS-Konfigurationsdatei definieren. Das IPQoS-System wählt die Verkehrswerte zur Verarbeitung aus, die den Filtern in seiner IPQoS-Konfigurationsdatei entsprechen. Siehe auch Paketfilter.

Firewall Ein Gerät oder eine Software, die das private Netzwerk oder Intranet eine Organisation vom Internet isoliert und es somit vor externen Eindringversuchen schützt. Eine Firewall kann Paketfilterung, Proxy-Server sowie NAT (Network Address Translation) enthalten.

Flow Accounting Bei IPQoS, der Prozess zum Erfassen und Aufzeichnen von Informationen zu Verkehrswerten. Sie richten das Flow Accounting ein, in dem Sie Parameter für das `flowacct`-Modul in der IPQoS-Konfigurationsdatei definieren.

Foreign-Agent Ein Router oder Server im Foreign-Netzwerk, das der mobile Knoten besucht.

Foreign-Netzwerk Ein Netzwerk, bei dem es sich nicht um das Home-Netzwerk des mobilen Knotens handelt.

Generic Routing Encapsulation (GRE) Eine optionale Form des Tunneling, das von Home-Agents, Foreign-Agents und mobilen Endgeräten unterstützt werden kann. GRE ermöglicht es, dass ein Paket eines beliebigen Protokolls auf der Netzwerkschicht in ein Zustellungspaket eines anderen (oder des gleichen) Protokolls auf der Netzwerkschicht eingekapselt wird.

Hash-Wert Eine Zahl, die aus einer Zeichenfolge generiert wird. Mithilfe von Hash-Funktionen wird sichergestellt, dass übertragene Nachrichten unverfälscht bleiben. MD5 und SHA-1 sind Beispiele für Einweg-Hash-Funktionen.

Header Siehe IP-Header.

HMAC Verschlüsselte Hashing-Methode zur Nachrichtenauthentifizierung. HMAC ist ein geheimer Schlüssel-Authentifizierungsalgorithmus. HMAC wird mit einer iterativen kryptografischen Hash-Funktion wie MD5 oder SHA-1 zusammen mit einem geheimen gemeinsam genutzten Schlüssel verwendet. Die kryptografischen Stärke von HMAC hängt von den Eigenschaften der zu Grunde liegenden Hash-Funktion ab.

Home-Adresse Eine IP-Adresse, die einem mobilen Endgerät für einen längeren Zeitraum zugewiesen wird. Diese Adresse bleibt gleich, auch wenn das Endgerät an einer anderen Stelle im Internet oder im Netzwerk der Organisation angeschlossen wird.

Home-Agent Ein Router oder Server im Home-Netzwerk eines mobilen Endgeräts.

Home-Netzwerk Ein Netzwerk, dessen Netzwerkpräfix dem Netzwerkpräfix der Home-Adresse eines mobilen Endgeräts entspricht.

Hop Ein Maß, mit dem die Anzahl an Routern zwischen zwei Hosts angegeben wird. Wenn auf dem Weg von der Quelle bis zum Ziel drei Router durchlaufen werden müssen, sind die Hosts vier Hops voneinander entfernt.

Host Ein System, das keine Paketweiterleitung durchführt. Nach Installation von Oracle Solaris wird ein System standardmäßig zu einem Host, das heißt, das System kann keine Pakete weiterleiten. In der Regel verfügt ein Host über eine physikalische Schnittstelle, obwohl er über mehrere Schnittstellen verfügen kann.

ICMP Internet Control Message Protocol. Dieses Protokoll dient zur Verarbeitung von Fehlern und zum Austausch von Steuerungsnachrichten.

ICMP Echo Request-Paket Ein Paket, das an einen Computer im Internet gesendet wird, um eine Anforderung abzurufen. Diese Pakete werden häufig als „Ping"-Pakete bezeichnet.

IKE Internet Key Exchange. IKE automatisiert die Bereitstellung von authentifiziertem Schlüsselmaterial für IPsec's Security Association (SA)s.

Internet Protocol (IP) Die Methode oder das Protokoll, mit dem Daten von einem Computer zu einem anderen im Internet gesendet werden.

IP Siehe Internet Protocol (IP), IPv4 und IPv6.

IP-Datagramm Ein Paket mit Informationen, dass über IP übertragen wird. Ein IP-Datagramm enthält einen Header und Daten. Der Header enthält die Adressen der Datagrammquelle und des Datagrammziels. Weitere Felder im Header helfen dabei, Daten in den begleitenden Datagrammen am Ziel zu identifizieren und zusammenzusetzen.

IP-Header Zwanzig Datenbytes, die ein Internetpaket eindeutig identifizieren. Der Header enthält die Quellen- und Zieladresse des Pakets. Es besteht eine Option, das dem Header weitere Byte hinzugefügt werden können.

IP in IP-Kapselung Der Mechanismus für das Tunneling von IP-Paketen in IP-Paketen.

IP-Link Eine Kommunikationsfunktion oder ein Medium, über das Endgeräte auf der Sicherungsschicht kommunizieren können. Die Sicherungsschicht ist die Schicht unmittelbar vor IPv4/IPv6. Beispiele sind Ethernets (einfach oder gebrückt) oder ATM-Netzwerke. Einem IP-Link sind eine oder mehrere IPv4-Teilnetznummern oder Präfixe zugeordnet. Eine Teilnetznummer oder ein Präfix kann nur einen IP-Link zugeordnet werden. Bei ATM LANE ist ein IP-Link ein einzelnes, emuliertes LAN. Wenn Sie das ARP verwenden, beträgt der Bereich des ARP-Protokolls einen IP-Link.

IP-Stack TCP/IP wird häufig als „Stack" bezeichnet. Dies bezieht sich auf die Ebenen (TCP, IP und manchmal andere), die alle Daten bei einem Datenaustausch auf Client und Server durchlaufen.

IPMP-Gruppe
IP Multipathing Group, besteht aus mehreren Netzwerkschnittstellen mit mehreren Datenadressen, die vom System als untereinander austauschbar behandelt, um die Netzwerkverfügbarkeit und -nutzung zu verbessern. Die IPMP-Gruppe, einschließlich aller zu Grunde liegenden IP-Schnittstellen und Datenadressen, wird durch eine IPMP-Schnittstelle dargestellt.

IPQoS
Eine Softwarefunktion, die eine Implementierung des Diffserv-Modell-Standards bereitstellt, plus Flow Accounting und 802.1 D-Markierung für virtuelle LANs. Mit IPQoS können Kunden und Anwendungen verschiedene Ebenen von Netzwerkservices bereitgestellt werden, die in der IPQoS-Konfigurationsdatei definiert sind.

IPsec
IP Security (IP-Sicherheit). Die Sicherheitsarchitektur, die den Schutz für IP-Datagramme bereitstellt.

IPv4
Internet Protocol, Version 4. IPv4 wird manchmal auch als IP bezeichnet. Diese Version unterstützt einen 32-Bit-Adressraum.

IPv6
Internet Protocol, Version 6. IPv6 unterstützt einen 128-Bit-Adressraum.

Kapselung
Ein Header und eine Nutzlast werden im ersten Paket platziert, das anschließend in die Nutzlast des zweiten Pakets eingefügt wird.

Klasse
Bei IPQoS eine Gruppe von Flüssen im Netzwerk mit ähnlichen Eigenschaften. Sie definieren Klassen in der IPQoS-Konfigurationsdatei.

Knoten
Bei IPv6 ein IPv6-konformes System, entweder ein Host oder ein Router.

Lastverteilung
Der Prozess, eingehenden und abgehenden Datenverkehr über mehrere Schnittstellen zu verteilen. Durch eine Lastverteilung wird ein höherer Durchsatz im Netzwerk erreicht. Eine Lastverteilung tritt nur ein, wenn der Netzwerkverkehr über mehrere Verbindungen an mehrere Ziele fließt. Es gibt zwei Arten der Lastverteilung: eingehende Lastverteilung für eingehenden Verkehr und abgehende Lastverteilung für abgehenden Datenverkehr.

Link-lokale Adresse
Bei IPv6 eine Bezeichnung, die zur Adressierung auf einem einzelnen Link z. B. für eine automatische Adresskonfiguration verwendet wird. In der Standardeinstellung wird die Link-lokale Adresse aus der MAC-Adresse des Systems erzeugt.

Local-use-Adresse
Eine Unicast-Adresse, die nur in einem lokalen Bereich routefähig ist (innerhalb des Teilnetzes oder innerhalb eines Abonnentennetzwerks). Diese Adresse kann auch lokal oder global einmalig sein.

Marker
1. Ein Modul in der Diffserv-Architektur und IPQoS, das das DS-Feld eines IP-Pakets mit einem Wert markiert, der angibt, wie das Paket weitergeleitet werden muss. In der IPQoS-Implementierung ist `dscpmk` das Markermodul.

2. Ein Modul in der IPQoS-Implementierung, das das virtuelle LAN-Tag eines Ethernet-Datagramms mit einem Wert für die Benutzerpriorität markiert. Der Benutzerprioritätswert kennzeichnet, wie Datagramme in einem Netzwerk mit VLAN-Geräten weitergeleitet werden müssen. Dieses Modul wird als `dlcosmk` bezeichnet.

MD5
Eine iterative kryptografische Hash-Funktionen, die zur Nachrichtenauthentifizierung, einschließlich digitaler Signaturen, verwendet wird. Diese Funktion wurde 1991 von Rivest entwickelt.

Message Authentication Code (MAC)
MAC bietet Zusicherung der Datenintegrität und authentifiziert den Datenursprung. MAC bietet keinen Schutz gegenüber Lauschangriffen.

Meter
Ein Modul in der Diffserv-Architektur, mit dem die Rate des Verkehrswerts für eine bestimmte Klasse gemessen wird. Die IPQoS-Implementierung umfasst zwei Meter, `tokenmt` und `tswtclmt`.

Minimale Kapselung
Eine optionale Form des IPv4 in IPv4-Tunneling, das von Home-Agents, Foreign-Agents und mobilen Endgeräten unterstützt werden kann. Die minimale Kapselung hat 8 oder 12 Byte weniger Overhead als eine IP in IP-Kapselung.

Mobiler Knoten
Ein Host oder Router, der seinen Anschlusspunkt von einem Netzwerk zu einem anderen ändern und alle vorhandenen Verbindungen mithilfe seiner IP-Home-Adresse beibehalten kann.

Mobility-Agent
Entweder ein Home-Agent oder ein Foreign-Agent.

Mobility-Bindung
Die Zuordnung einer Home-Adresse zu einer Care-Of-Adresse, zusammen mit einer verbleibenden Lebensdauer für diese Zuordnung.

Mobility Security Association
Eine Sammlung von Sicherheitsmaßnahmen, z. B. ein Authentifizierungsalgorithmus, zwischen einem Knotenpaar, die an den Mobile IP-Protokollnachrichten angewendet werden, die zwischen den beiden Knoten ausgetauscht werden.

MTU
Maximum Transmission Unit. Die Größe (in Oktetten), die über einen Link übertragen werden kann. Beispielsweise lautet die MTU bei Ethernet 1500 Oktette.

Multicast-Adresse
Eine IPv6-Adresse, die eine Schnittstellengruppe auf besondere Weise identifiziert. Ein Paket, das an eine Multicast-Adresse gesendet wird, wird allen Schnittstellen in dieser Gruppe zugestellt. Die IPv6 Multicast-Adresse hat ähnliche Funktionen wie die IPv4 Broadcast-Adresse.

Multihomed Host
Ein System, das über mehrere physikalische Schnittstellen verfügt und keine Paketweiterleitung durchführt. Ein Multihomed Host kann Routing-Protokolle ausführen.

NAT
Siehe Network Address Translation.

Neighbor Advertisement-Nachricht
Eine Antwort auf eine Neighbor Solicitation-Nachricht oder der Vorgang, wenn ein Knoten unbeantwortete Neighbor Advertisement-Nachrichten sendet, um die Änderung einer Sicherungsschichtadresse bekannt zu geben.

Neighbor Discovery
Ein IP-Mechanismus, der als Hosts ermöglicht, andere Hosts zu lokalisieren, die sich auf einem angeschlossenen Link befinden.

Neighbor Solicitation
Solicitation-Nachrichten werden von einem Knoten gesendet, um die Sicherungsschichtadresse eines Neighbors zu ermitteln. Eine Neighbor Solicitation stellt darüber hinaus sicher, ob ein Neighbor noch immer über eine zwischengespeicherte Sicherungsschichtadresse erreichbar ist.

Network Access Identifier (NAI) Eine Bezeichnung im Format „Benutzer@Domäne“, die den mobilen Knoten eindeutig identifiziert.

Network Address Translation NAT. Die Übersetzung einer IP-Adresse, die in einem Netzwerk verwendet wird, in eine andere IP-Adresse, die in einem anderen Netzwerk bekannt ist. Diese Funktion dient dazu, die Anzahl an erforderlichen globalen IP-Adressen einzuschränken.

Netzwerkschnittstellenkarte (NIC) Eine Netzwerk-Adapterkarte, die als Schnittstelle in einem Netzwerk dient. Einige NICs verfügen über mehrere physikalische Schnittstellen, zum Beispiel die `qfe`-Karte.

Nutzlast Die Daten, die in einem Paket übertragen werden. Die Nutzlast umfasst nicht die Header-Informationen, die erforderlich sind, um das Paket an sein Ziel zu leiten.

Paket Eine Gruppe mit Informationen, die als eine Einheit über Kommunikationsleitungen übertragen wird. Enthält einen IP-Header sowie eine Nutzlast.

Paket-Header Siehe IP-Header.

Paketfilter Eine Firewallfunktion, die so konfiguriert werden kann, dass sie bestimmte Pakete passieren lässt oder abweist.

Per-Hop-Behavior (PHB) Eine Priorität, die einer Verkehrsklasse zugewiesen wird. Das PHB gibt die Prioritätsstufe an, die Datenflüsse dieser Klasse in Relation zu anderen Verkehrsklassen aufweisen.

Perfect Forward Secrecy (PFS) Bei PFS kann der Schlüssel, der zum Schützen der Datenübertragung verwendet wird, nicht zum Ableiten weiterer Schlüssel verwendet werden. Außerdem wird die Quelle des Schlüssels, der zum Schützen von Datenübertragungen verwendet wird, niemals zum Ableiten weiterer Schlüssel verwendet.

PFS gilt nur für authentifizierten Schlüsselaustausch. Siehe auch Diffie-Hellman-Protokoll.

Physikalische Schnittstelle Die Verbindung eines Systems mit einem Link. Diese Verbindung wird häufig als Gerätetreiber plus Netzwerkschnittstellenkarte (NIC) implementiert. Einige NICs haben mehrere Anschlusspunkt, z. B. `qfe`.

PKI Public Key Infrastructure. Ein System digitaler Zertifikate, Zertifizierungsstellen und anderen Registrierungsbehörden, das die Gültigkeit jeder an einer Internet Transaktionen beteiligten Partei prüft und authentifiziert.

plumb Das Anmelden eines Gerätes, das einem physikalischen Schnittstellennamen zugeordnet ist, beim Systemkernel. Wenn eine Schnittstelle geplumbt wurde, werden die Datenströme so eingerichtet, dass das Gerät vom IP-Protokoll verwendet werden kann. Das Plumbing einer Schnittstelle während der aktuellen Sitzung erfolgt mit dem Befehl `ifconfig`.

Private Adresse Eine IP-Adresse, die nicht über das Internet routefähig ist. Private Adressen können von internen Netzwerken auf Hosts verwendet werden, die keine Internet-Konnektivität benötigen. Diese Adressen sind unter Address Allocation for Private Internets (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`) definiert und werden oft als „1918”-Adressen bezeichnet.

Protokollstapel Siehe IP-Stack.

Proxy-Server Ein Server zwischen einer Client-Anwendung (z. B. einem Webbrowser) und einem anderen Server. Der Proxy-Server dient zum Filtern von Anforderungen, beispielsweise um den Zugriff auf bestimmte Websites zu verhindern.

PublicKey-Kryptographie Ein Kryptographiesystem, das zwei unterschiedliche Schlüssel verwendet. Der PublicKey ist in jedem bekannt. Der PrivateKey ist nur dem Empfänger der Nachricht bekannt. IKE stellt PublicKeys für IPsec bereit.

Registrierung Der Prozess, bei dem ein mobiler Knoten seine Care-Of-Adresse bei seinem Home-Agent und dem Foreign-Agent registriert, wenn er sich nicht in einem Home-Netzwerk befindet.

Reparaturerkennung Der Prozess, bei dem erkannt wird, dass eine NIC oder der Pfad von einer NIC zu einem Gerät auf der Schicht 3 nach einem Ausfall wieder ordnungsgemäß funktioniert.

Replay Bei IPsec ein Angriff, bei dem ein Paket von einem Eindringling erfasst wird. Das gespeicherte Paket ersetzt oder wiederholt das Original dann zu einem späteren Zeitpunkt. Zum Schutz vor solchen Angriffen kann ein Paket ein Feld enthalten, das die Lebensdauer des geheimen Schlüssels erhöht, der das Paket schützt.

Router Ein System, das in der Regel über mehrere Schnittstellen verfügt, Routing-Protokolle ausführt und Pakete weiterleitet. Sie können ein System mit nur einer Schnittstelle als Router konfigurieren, wenn es sich bei dem System um den Endpunkt einer PPP-Link handelt.

Router Advertisement Der Prozess, bei dem Router ihr Vorhandensein zusammen mit verschiedenen Link- und Internet-Parametern entweder regelmäßig oder als Antwort auf eine Router Solicitation-Nachricht senden.

Router Discovery Der Prozess, bei dem Hosts Router erfassen, die sich auf dem angeschlossenen Link befinden.

Router Solicitation Der Prozess, bei dem Hosts auffordern, sofort und nicht erst zur nächsten geplanten Zeit Router Advertisement-Nachrichten zu generieren.

RSA Eine Methode zum Beziehen digitaler Signaturen und PublicKey-Kryptosystemen. Diese Methode wurde zuerst 1978 von seinen Entwicklern Rivest, Shamir und Adleman beschrieben.

Rücktunnel Ein Tunnel, der an der Care-Of-Adresse des mobilen Knotens beginnt und am Home-Agent endet.

SA Siehe Security Association (SA).

SADB Security Associations-Datenbank. Eine Tabelle, die kryptographische Schlüssel und kryptographische Algorithmen festlegt. Die Schlüssel und Algorithmen werden bei der sicheren Datenübertragung verwendet.

Schlüsselmanagement Das Verfahren zum Verwalten der Security Association (SA)s.

Schlüsselspeichername Der Name, den ein Administrator dem Speicherbereich (oder Schlüsselspeicher) auf einer Netzwerkschnittstellenkarte (NIC) gegeben hat. Der Schlüsselspeichername wird auch als Token oder die Token-ID bezeichnet.

SCTP Siehe Streams Control Transport-Protokoll.

Security Association (SA) Eine Zuordnung, die Sicherheitseigenschaften von einem Host an einen zweiten Host weitergibt.

Security Parameter Index (SPI) Eine ganze Zahl, mit der die Reihe in der Security Associations-Datenbank (SADB) angegeben wird, die ein Empfänger zum Entschlüsseln eines empfangenen Pakets verwenden soll.

Security Policy-Datenbank (SPD) Datenbank, in der die Schutzebene angegeben ist, die für ein bestimmtes Datenpaket gilt. Die SPD filtert IP-Verkehr, um festzustellen, ob ein Paket verworfen, im Klartext weitergeleitet oder mit IPsec geschützt werden muss.

Selektor Das Element, das Kriterien festlegt, die an Paketen einer bestimmten Klasse angewendet werden müssen, um Verkehr dieser Klasse aus dem Netzwerkstrom zu wählen. Sie definieren Selektoren in der filter-Klausel der IPQoS-Konfigurationsdatei.

SHA-1 Secure Hashing Algorithm. Dieser Algorithmus arbeitet mit jeder Eingabelänge kleiner als 2^{64}, um einen Nachrichtendigest zu erzeugen. Der SHA-1-Algorithmus ist die Eingabe für DSA.

Sicherungsssschicht Die Schicht unmittelbar unterhalb IPv4/IPv6.

Smurf-Angriff Das Verwenden von ICMP Echo Request-Paketen, die von remoten Standorten an eine IP Broadcast-Adresse oder an mehrere Broadcast-Adressen gesendet werden und starke Netzwerküberlasung oder -ausfälle erzeugen können.

Sniff Lauschangriff auf Computernetzwerke – werden häufig im Rahmen von automatisierten Programmen verwendet, um Informationen (z. B. Passwörter im Klartext) am Kabel abzugreifen.

SPD Siehe Security Policy-Datenbank (SPD).

SPI Siehe Security Parameter Index (SPI).

Spoof Spoofing ist das Erlangen von nicht autorisiertem Zugriff auf einen Computer, indem eine Nachricht mit eine IP-Adresse an den Computer gesendet und vorgetäuscht wird, sie käme von einem vertrauenswürdigen Host. Für das IP-Spoofing muss ein Hacker zunächst zahlreiche verschiedene Techniken anwenden, um die IP-Adresse eines vertrauenswürdigen Host in Erfahrung zu bringen und dann die Paket-Header modifizieren, so dass das Paket von diesem Host zu kommen scheint.

Stack Siehe IP-Stack.

Standby Eine physikalische Schnittstelle, die nicht zur Übertragung von Datenverkehr verwendet wird, es sei denn, eine andere physikalische Schnittstelle fällt aus.

Standort-lokale use-Adresse Eine Bezeichnung, die zur Adressierung an einem einzelnen Standort verwendet wird.

Statusbehafteter Paketfilter Ein Paketfilter kann den Status aktiver Verbindungen überwachen und anhand der bezogenen Informationen festlegen, welche Netzwerkpakete eine Firewall passieren dürfen. Durch das Verfolgen und Vergleichen von Anforderungen und Antworten kann ein statusbehafteter Filter nach einer Antwort suchen, die keiner Anforderung entspricht.

Statusfreie automatische Konfiguration Der Prozess, bei dem ein Host seine eigenen IPv6-Adressen erzeugt, indem er seine MAC-Adresse und einen IPv6-Präfix kombiniert, der von einem lokalen IPv6-Router bekannt gegeben wird.

Stream Control Transport-Protokoll Ein Protokoll auf der Transportschicht, das verbindungsorientierte Kommunikation ähnlich dem TCP bietet. Darüber hinaus unterstützt SCTP Multihoming, bei dem einer der Endpunkte einer Verbindung über mehrere IP-Adressen verfügen kann.

Symmetrische Schlüssel-Kryptographie Ein Verschlüsselungssystem, bei dem Sender und Empfänger einer Nachricht einen einzelnen allgemeinen Schlüssel verwenden. Dieser allgemeine Schlüssel dient zur Verschlüsselung und Entschlüsselung der Nachricht. Symmetrische Schlüssel dienen zum Verschlüsseln der Datenübertragung in IPsec. DES ist ein Beispiel für ein symmetrisches Schlüsselsystem.

TCP/IP TCP/IP (Transmission Control Protocol/Internet Protocol) ist die allgemeine Kommunikationssprache oder das allgemeine Kommunikationsprotokoll im Internet. Es kann auch als Kommunikationsprotokoll in einem privaten Netzwerk verwendet werden (entweder in einerm Intranet oder einem Extranet).

Testadresse Eine IP-Adresse in einer IPMP-Gruppe, die als Quell- oder Zieladresse für Stichproben verwendet werden muss, aber nicht als Quell- oder Zieladresse für Datenverkehr verwendet werden darf.

Triple-DES Triple-Data Encryption Standard. Eine Verschlüsselungsmethode mit symmetrischen Schlüsseln. Triple-DES erfordert eine Schlüssellänge von 168 Bit. Triple-DES wird als 3DES geschrieben.

Tunnel Der Pfad, dem ein Datagramm folgt, solange es eingekapselt ist. Siehe auch Kapselung.

Umleitung Eine Umleitung ermöglicht es einem Router, einen Host über einen Knoten im ersten Hop zu informieren, über den ein bestimmtes Ziel besser erreicht werden kann.

Unicast-Adresse Eine IPv6-Adresse, die als eine einzelne Schnittstelle eines IPv6-konformen Knoten identifiziert wird. Die Komponenten einer Unicast-Adresse sind das Standortpräfix, Teilnetz-ID und Schnittstellen-ID.

Virtual LAN (VLAN)-Gerät Netzwerkschnittstellen, die Verkehrsweiterleitung auf der Ethernet-Schicht (Übertragungssicherungsschicht) des IP-Protokollstapel bereitstellen.

Virtuelle Netzwerkschnittstelle (virtual network interface, VNIC) Eine Pseudo-Schnittstelle, die unabhängig davon, ob sie in einer physischen Netzwerkschnittstelle konfiguriert ist oder nicht, virtuelle Netzwerkkonnektivität bereitstellt. Container wie z. B. exklusive IP-Zonen oder xVM-Domänen werden eine Schicht über virtuellen Netzwerkschnittstellen konfiguriert und bilden so ein virtuelles Netzwerk.

Virtuelles Netzwerk Verschiedene Software- und Hardware-Netzwerkressourcen und Funktionalitäten, die zusammen als einzige Software-Entität verwaltet werden. Ein *internes* virtuelles Netzwerk konsolidiert Netzwerkressourcen in ein einziges System, das manchmal als „Netzwerk in der Box" bezeichnet wird.

Virtuelles privates Netzwerk (VPN) Ein einzelnes, sicheres, logisches Netzwerk, das Tunnel durch öffentliche Netzwerke wie das Internet verwendet.

Vorwärtstunnel Ein Tunnel, der bei Home-Agent beginnt und an der Care-Of-Adresse des mobilen Endgeräts endet.

Zertifikat-Rücklnahmeliste (Certificate revocation list, CRL) Eine Liste der PublicKey-Zertifikate, die von einer CA zurückgenommen wurden. CRLs sind in der CRL-Datenbank gespeichert, die von der IKE gepflegt wird.

Zertifizierungsstelle (Certificate authority, CA) Eine vertrauenswürdige Drittorganisation und ein Unternehmen, das digitale Zertifikate ausgibt, die für digitale Signaturen und PublicKey-PrivateKey-Paare verwendet werden. Die CA garantiert die Identität der Person, der das einmalige Zertifikat gewährt wurde.

Index

Zahlen und Symbole
* (Sternchen), -Platzhalter in
  bootparams-Datenbank, 270
>-Eingabeaufforderung, ipseckey-Befehlsmodus, 546
3DES-Verschlüsselungsalgorithmen, IPsec und, 523
3DES-Verschlüsselungsalgorithmus,
  Schlüssellänge, 547
6to4-Adresse
  Format, 278
  Hostadresse, 279
6to4-Advertisement-Nachrichten, 210
6to4-Präfix
  Erklärung der Komponenten, 279
  /etc/inet/ndpd.conf-Advertisement, 210
6to4-Pseudoschnittstellenkonfiguration, 208
6to4-Relay-Router
  Aufgaben bei der Tunnelkonfiguration, 211, 213
  in einem 6to4-Tunnel, 291
  Sicherheitsbetrachtungen, 250, 314-316
  Tunneltopologie, 315
6to4-Routerkonfiguration
  Aufgaben, 208
  Beispiele, 210
6to4-Tunnel
  6to4-Relay-Router, 211
  Beispieltopologie, 312
  bekannte Probleme, 251
  Definition, 208
  Paketfluss, 314, 315
6to4relay-Befehl, 212
  Aufgaben bei der Tunnelkonfiguration, 212
  Beispiele, 291
6to4relay-Befehl *(Fortsetzung)*
  Definition, 291
  Syntax, 291

A
-A-Option
  ikecert-Befehl, 662
  ikecert certlocal-Befehl, 625
-a-Option
  ikecert-Befehl, 637
  ikecert certdb-Befehl, 627, 632
  ikecert certrldb-Befehl, 642
  ipsecconf-Befehl, 539
AAAA-Datensätze, 215, 316
Abgeworfene oder verlorene Pakete, 41, 233
acctadm-Befehl, für das Flow Accounting, 920
acctadm-Befehl, für Flow Accounting, 834, 904
ACK-Segment, 47
action-Anweisung, 921
Address-Abschnitt
  Label und Werte, 770
  Mobile IP-Konfigurationsdatei, 768, 770-773
  NAI, Label und Werte, 771
  Node-Default, Label und Werte, 773
  private Adressen, 770, 771
Address Resolution Protocol (ARP)
  Definition, 41
  Vergleich mit Neighbor
    Discovery-Protokoll, 304-306
Administrative Unterbereiche, 68

Administratives Modell, 455
Adressauflösung, in IPv6, 85
Adressen
  6to4-Format, 278
  Adressen aller Schnittstellen anzeigen, 224
  CIDR-Format, 62
  Datenadressen, IPMP, 784
  Ethernet-Adressen
    `ethers`-Datenbank, 266, 270
  globale IPv6-Unicast-Adresse, 81-82
  IPv4-Format, 61
  IPv4-Netzmaske, 261
  IPv6, 6to4-Format, 208
  IPv6 Link-lokal, 83
  Loopback-Adresse, 257
  Multicast, in IPv6, 280-281
  Standard-Adressauswahl, 242-245
  temporär, in IPv6, 196-199
  Testadressen, IPMP, 784-786
Adresspools
  anhängen, 706
  anzeigen, 705
  entfernen, 705-706
  konfigurieren, 675-677
  Statistiken anzeigen, 709-710
  Übersicht, 675-677
`Advertisements`-Abschnitt
  Label und Werte, 765
  Mobile IP-Konfigurationsdatei, 765-767
`AdvertiseOnBcast`-Label, 746, 766
`AdvFrequency`-Label, 746, 766
`AdvInitCount`-Label, 766
`AdvLifetime`-Label, 746, 750, 766
`AdvLimitUnsolicited`-Label, 767
AES-Verschlüsselungsalgorithmen, IPsec und, 523
Agent Advertisement-Nachrichten
  Mobile IP, 729
  über dynamische Schnittstellen, 730, 765
Agent-Erkennung, Mobile IP, 729-730
Agent Solicitation, Mobile IP, 728, 729, 730
Aggregationen
  Anforderungen, 177
  bearbeiten, 179-180
  Definition, 173
Aggregationen *(Fortsetzung)*
  erstellen, 177-179
  Funktionen, 173
  Richtlinie zum Lastenausgleich, 176
  Schnittstellen entfernen, 181
  Topologien
    Back-to-Back, 175
    Basis-, 174
    mit Switch, 174
AH, *Siehe* Authentication Header (AH)
aktiv-aktive Schnittstellenkonfiguration, IPMP, 788
Aktiv-Standby-Schnittstellenkonfiguration, IPMP, 788
Aktive Regelliste, *Siehe* Oracle Solaris IP Filter
Aktivieren von Oracle Solaris IP Filter, in früheren
  Oracle Solaris 10-Versionen, 688-691
Aktualisieren, PresharedKeys (IKE), 616-617
Ändern
  DHCP-Makros, 422
  DHCP-Optionen, 436
Ändern der IKE-Übertragungsparameter (Übersicht
  der Schritte), 654
Anonymer Anmeldename, 43
Anonymes FTP, Programm, Beschreibung, 43
Anwendungsschicht
  OSI, 38
  Paket-Lebenszyklus
    empfangender Host, 49
    sendender Host, 46
  TCP/IP, 42, 45
    Beschreibung, 39, 42, 43
    Dateiservices, 45
    Namen-Services, 44
    Netzwerkverwaltung, 45
    Routing-Protokolle, 45
    standardmäßige TCP/IP-Services, 43
    UNIX „r“-Befehle, 44
Anwendungsserver, für IPQoS konfigurieren, 880
anycast-Adressen, 212
Anycast-Adressen, Definition, 84
anycast-Gruppen, 6to4-Relay-Router, 212
Anzeigen
  IPsec-Konfiguration, 595-596
  IPsec-Richtlinie, 542-543
Assured Forwarding (AF), 837, 914

Assured Forwarding (AF) *(Fortsetzung)*
AF Codepoints-Tabelle, 914
für die Marker `action`-Anweisung, 874
ATM, IPMP-Unterstützung für, 801
ATM-Unterstützung, IPv6 über, 318
Aufgabe
IPQoS
Konfigurationen planen, 841
Ausfall einer Gruppe, IPMP, 791
Ausfallerkennung, in IPMP, 789
bei einem Systemstart fehlende NICs, 795-796
Definition, 782
Stichprobenrate, 780
`auth_algs`-Sicherheitsoption, `ifconfig`-Befehl, 600
Authentication Header (AH)
IP-Datagramm schützen, 520-521
IP-Pakete schützen, 513
IPsec-Schutzmechanismus, 520-524
Sicherheitsbetrachtungen, 522
Authentifizierungsalgorithmen
für IPsec angeben, 600
IKE-Zertifikate, 662
Automatische Adresskonfiguration
auf einem IPv6-Knoten aktivieren, 187, 188, 190
Definition, 85, 86-87
IPv6, 296, 300
Automatische Tunnel, Übergang zu IPv6, 309
Autonomes System (AS), *Siehe* Netzwerktopologie

B

Bandbreitenregulierung, Planung, in der QoS-Richtlinie, 849
`BaseAddress`-Label, 747, 769
Befehl `routeadm`, Konfigurieren von VPN mit IPsec, 582
Befehle
IKE, 660-664
`ikeadm`-Befehl, 609, 658, 659-660
`ikecert`-Befehl, 609, 658, 660
`in.iked`-Daemon, 658
IPsec
`in.iked`-Befehl, 520
`ipsecalgs`-Befehl, 523, 597
Befehle, IPsec *(Fortsetzung)*
`ipsecconf`-Befehl, 531, 539, 594-595
`ipseckey`-Befehl, 531, 546, 598-599
Liste, 530-532
Sicherheitsbetrachtungen, 598-599
`snoop`-Befehl, 599, 601
Benutzerpriorität-Wert, 833
Berechnungen
IKE auf der Hardware beschleunigen, 608
IKE in Hardware beschleunigen, 651-652, 652-654
Beschleunigen, IKE-Berechnungen, 651
Beschleunigung, IKE-Berechnungen, 608
Besucherliste
Foreign-Agent, 756
Mobile IP, 774
BGP, *Siehe* Routing-Protokolle
Bibliotheken, PKCS #11, 662
Binär-Dezimal-Umwandlung, 262
Bindungstabelle
Home-Agent, 756, 757
Mobile IP, 774
Bitübertragungsschicht (OSI), 39
Bitübertragungsschicht (TCP/IP), 40, 48
Blowfish-Verschlüsselungsalgorithmen, IPsec und, 523
Booten, Netzwerkkonfigurationsserver, Boot-Protokolle, 104
BOOTP-Protokoll
Clients mit DHCP-Service unterstützen, 399
und DHCP, 321
BOOTP-Relay-Agent
Hops, 386
Konfiguration
mit DHCP Manager, 360
mit `dhcpconfig -R`, 365
`bootparams`-Datenbank
entsprechende Namen-Service-Dateien, 267
Platzhaltereintrag, 270
Übersicht, 269
Bootparams-Protokoll, 105
Broadcast-Adresse, 768
Broadcast-Datagramme, Mobile IP, 739
BSD-basierte Betriebssysteme
`/etc/inet/hosts`-Dateiverknüpfung, 256

BSD-basierte Betriebssysteme *(Fortsetzung)*
  /etc/inet/netmasks-Dateiverknüpfung, 263

C

-c-Option
  in.iked-Daemon, 615
  ipsecconf-Befehl, 512, 595
  ipseckey-Befehl, 512, 598
Care-Of-Adresse
  beziehen, 730-731
  co-located, 728, 730, 736, 739
  Foreign-Agent, 730, 734, 737
  gemeinsam nutzen, 730
Care-of-Adresse, Mobile IP, 724
Care-Of-Adresse
  Mobility-Agents, 726
  Registrierung eines mobilen Knotens, 734
  Standort des mobilen Knotens, 726
  Statusinformationen, 775
cert_root-Schlüsselwort
  IKE-Konfigurationsdatei, 633, 639
cert_trust-Schlüsselwort
  IKE-Konfigurationsdatei, 628, 638
  ikecert-Befehl und, 662
Certificate Revocation Lists
  (Zertifikatrücknahmelisten), *Siehe* CRLs
Challenge-Label, 746, 768
class-Klausel, in der IPQoS-Konfigurationsdatei, 869
class-Klausel, in der IPQoS-Konfigurationsdatei, 923
classes, Liste der Selektoren, 908
Classifier-Modul, 831
  action-Anweisung, 868
  Funktionen des Classifiers, 908
Client-ID, 455
Clientkonfiguration, 455
Co-located Care-Of-Adresse, 728, 736, 739
  beziehen, 730
Computer, Kommunikation schützen, 535-539
CRC (cyclical redundancy check), Feld, 48
CRLs
  ignorieren, 634
  ike/crls-Datenbank, 664
  ikecert certrldb-Befehl, 663
CRLs *(Fortsetzung)*
  Liste, 641
  von einem zentralen Speicherort aus zugreifen, 640
cyclical redundancy check (CRC), Feld, 48

D

-D-Option
  ikecert-Befehl, 662
  ikecert certlocal-Befehl, 625
Daemons
  in.iked-Daemon, 604, 609, 658
  in.mpathd-Daemon, 780-781
  in.ndpd-Daemon, 296
  in.ripngd Daemon, 193
  in.ripngd-Daemon, 297
  in.routed-Routing-Daemon, 141
  in.tftpd-Daemon, 112
  inetd Internet Services, 263
  Netzwerkkonfigurationsserver, 112
  Netzwerkkonfigurationsserver,
    Boot-Protokolle, 104
Darstellungsschicht (OSI), 38
Datagramme
  Formatierung im IP-Protokoll, 40
  Funktionen des UDP-Protokolls, 42
  IP, 513
  IP-Header, 48
  Paketprozess, 48
Dateien
  IKE
    crls-Verzeichnis, 609, 664
    ike/config-Datei, 531, 606, 609, 658
    ike.preshared-Datei, 609, 660
    ike.privatekeys-Verzeichnis, 609, 663
    publickeys Verzeichnis, 663
    publickeys-Verzeichnis, 609
  IPsec
    ipsecinit.conf-Datei, 530, 595-596
    ipseckeys-Datei, 531
Dateiservices, 45
Datenadressen, IPMP, Definition, 784
Datenbanken
  IKE, 660-664

Datenbanken *(Fortsetzung)*
ike/crls-Datenbank, 663, 664
ike.privatekeys-Datenbank, 661, 663
ike/publickeys Datenbank, 663
ike/publickeys-Datenbank, 662
Security Policy-Datenbank (SPD), 513
Sicherheitszuordnung-Datenbank (SADB), 597
Datenkapselung
Definition, 45
und der TCP/IP-Protokollstapel, 45, 49
Datenkommunikation, 45, 49
Paket-Lebenszyklus, 46, 49
Datenverkehr-Konformität
Planung
Ergebnisse in der QoS-Richtlinie, 854
Raten in der QoS-Richtlinie, 853
Datenverkehr weiterleiten,
Datagrammweiterleitung, 915
Datenverkehrkonformität
Definition, 887
rate-Parameter, 910, 911
Datenverkehrskonformität, Ergebnis, 910
Deaktivieren von Oracle Solaris IP Filter, 692-694
defaultdomain-Datei
Beschreibung, 255
für den Netzwerkclient-Modus löschen, 114
lokale Dateien-Modus konfigurieren, 111
defaultrouter-Datei
automatische Router-Protokoll-Auswahl und, 139
Beschreibung, 255
lokale Dateien-Modus konfigurieren, 111
deprecated-Attribut, ifconfig-Befehl, 786
DES-Verschlüsselungsalgorithmen, IPsec und, 523
Dezimal-Binär-Umwandlung, 262
DHCP-Befehlszeilenprogramme, 330
Berechtigungen, 371
DHCP-Client
Administration, 463
aktivieren, 462-463
auf laufwerkslosen Clientsystemen, 440
Client-ID, 405
deaktivieren, 463
Definition, 336
dekonfigurieren, 463

DHCP-Client *(Fortsetzung)*
Ereignisskripten, 473-476
Fehlerbehebung, 484
herunterfahren, 461
Hostname
angeben, 468
Hostnamen erzeugen, 347
im Debugging-Modus ausführen
Beispielausgabe, 486
IP-Adresse abwerfen, 464
IP-Adresse freigegeben, 464
Leasing-Zeit verlängern, 464
logische Schnittstellen, 466
mehrere Netzwerkschnittstellen, 466
Namen-Services, 385
Netzwerkinformationen ohne Leasing, 442-443, 464
Optionsinformationen, 439
Parameter, 465-466
Programme ausführen mit, 473-476
Schnittstelle testen, 464
Schnittstellenstatus anzeigen, 465
starten, 458, 464
ungenaue Konfiguration, 493
DHCP-Datenspeicher
auswählen, 343
Daten exportieren, 448
Daten importieren, 450
Daten zwischen Servern verschieben, 446-452
importierte Daten ändern, 451, 452
konvertieren, 443-445
Übersicht, 327
DHCP-Datenspeicher konvertieren, 443-445
DHCP-Ereignisse, 473-476
DHCP-Konfigurationsassistent
Beschreibung, 356
für BOOTP-Relay-Agent, 361
DHCP-Leasing
Ablaufdatum, 406
aushandeln, 345
dynamisch und permanent, 349
reservierte IP-Adresse, 406
Richtlinie, 345
Typ, 406

DHCP-Leasing *(Fortsetzung)*
  und reservierte IP-Adressen, 350
  Zeit, 345
DHCP-Makros
  ändern, 422
  arbeiten mit, 419
  automatische Verarbeitung, 334
  erstellen, 426
  Gebietsschema-Makro, 357
  Größenbeschränkung, 336
  Kategorien, 334
  konfigurieren, 404
  löschen, 429
  Makro für Clientklassen, 335
  Makro für Netzwerkadresse, 335, 358
  Makros für Client-IDs, 335
  Netzwerk-Booten, 441
  Reihenfolge der Verarbeitung, 335
  Servermakro, 358
  Standard, 348
  Übersicht, 334
DHCP Manager
  Beschreibung, 329
  Fenster und Registerkarten, 368
  Funktionen, 352
  Menüs, 370
  starten, 370
  stoppen, 371
DHCP-Netzwerkassistent, 391
DHCP-Netzwerke
  ändern, 394
  arbeiten mit, 388-399
  aus dem DHCP-Service entfernen, 397
  zum DHCP-Service hinzufügen, 391
DHCP-Netzwerktabellen
  beim Dekonfigurieren löschen, 362
  Beschreibung, 329
  während der Serverkonfiguration erstellte, 358
DHCP-Optionen
  ändern, 436
  arbeiten mit, 430
  Eigenschaften, 431
  erstellen, 433
  löschen, 438

DHCP-Optionen *(Fortsetzung)*
  Übersicht, 333
DHCP-Protokoll
  Reihenfolge der Ereignisse, 323
  Übersicht, 321
  Vorteile in der Oracle Solaris-Umsetzung, 322
DHCP-Server
  Anzahl der zu konfigurierenden Server, 339
  auswählen, 343
  Datenspeicher, 327
  Fehlerbehebung, 477
  Funktionen, 326
  im Debugging-Modus ausführen
    Beispielausgabe, 487-490
  in Debugging-Modus ausführen, 485
  Konfiguration
    `dhcpconfig`-Befehl, 364
    gesammelte Informationen, 340
    mit DHCP Manager, 356
    Übersicht, 332
  Optionen, 375
    DHCP Manager, 387
    `dhcpconfig`-Befehl, 387-388
  Planung für mehrere Server, 350
  Verwaltung, 327
  zum Aktualisieren von DNS aktivieren, 382-383
DHCP-Service
  aktivieren und deaktivieren
    Auswirkungen, 372
    DHCP Manager, 373
    `dhcpconfig`-Befehl, 374
  BOOTP-Clients unterstützen, 399
  Cache-Angebotszeit, 386
  dekonfigurieren, 361
  Dekonfigurieren
    mit DHCP Manager, 363
  Fehlermeldungen, 481, 489
  IP-Adressen
    Eigenschaften ändern, 410
    für Client reservieren, 416
    hinzufügen, 406
    löschen, 413
    nicht verwendbar, 413
  IP-Adressen zuweisen, 333

DHCP-Service *(Fortsetzung)*
Netzwerke hinzufügen zum, 391
Netzwerkkonfiguration, Übersicht, 333
Netzwerkschnittstelle überwachen, 389
Netzwerktopologie, 338
Oracle Solaris-Netzwerkbooten und -installation, 440
Planung, 337
Protokollierung
Transaktionen, 378
Übersicht, 377
Service Management Facility, 374-375
Service-Optionen bearbeiten, 375
starten und stoppen
Auswirkungen, 372
DHCP Manager, 373
Unterstützung der WAN-Boot-Installation, 440
`dhcpagent`-Daemon, 458
Debugging-Modus, 484-485
Parameterdatei, 505
`dhcpconfig`-Befehl
Beschreibung, 331, 497
`dhcpinfo`-Befehl, Beschreibung, 498
`dhcpmgr`-Befehl, Beschreibung, 498
`dhcpsvc.conf`-Datei, 504
`dhcptab`-Tabelle, 357
automatisch einlesen, 386
beim Dekonfigurieren löschen, 362
Beschreibung, 504
Übersicht, 328
`dhcptags`-Datei, 506
DHCPv4-Client, Netzwerkschnittstelle verwalten, 460
DHCPv4 im Vergleich mit DHCPv6, 454
DHCPv6, Clientname, 455
DHCPv6, administratives Modell, 455
DHCPv6-Client, Netzwerkschnittstelle verwalten, 460
DHCPv6 im Vergleich mit DHCPv4, 454
`dhtadm`-Befehl
Beschreibung, 331, 497
Makros ändern mit, 422
Makros erstellen mit, 426
Makros löschen mit, 429
Optionen ändern mit, 436
Optionen erstellen mit, 433
`dhtadm`-Befehl *(Fortsetzung)*
Optionen löschen mit, 438
Differentiated Services, 825
Differentiated Services-Modell, 831
Netzwerktopologien, 842
unterschiedliche Serviceklassen bereitstellen, 830
Diffserv-konformer Router
DS Codepoints auswerten, 915
Planung, 847
Diffserv-Modell
Classifier-Modul, 831
Flow-Beispiel, 834
IPQoS-Implementierung, 831, 833, 834
Markermodule, 833
Metermodule, 833
Digitale Signaturen
DSA, 662
RSA, 662
`dladm`, Befehl
Modifizieren einer Aggregation, 180
Schnittstellen aus einer Aggregation entfernen, 181
Überprüfen des Aggregationsstatus, 178
zum Erstellen einer Aggregation, 177
`dladm`-Befehl
Status anzeigen, 158
VLAN konfigurieren, 171-173
`dlcosmk`-Marker, 833
Benutzerprioritätswerte, Tabelle, 916
Datagrammweiterleitung planen, 856
VLAN-Tags, 916
Domain-Namen
`/etc/defaultdomain`-Datei, 111
Registrierung, 38
Domain-Namen-System (DNS)
als Namen-Service auswählen, 67
Beschreibung, 44
Domain-Namen-Registrierung, 38
dynamische Aktualisierungen durch DHCP-Server aktivieren, 382-383
Erweiterungen für IPv6, 316
IPv6-Unterstützung vorbereiten, 96
Netzwerkdatenbanken, 67, 265
Reverse Zone-Datei, 214
Zone-Datei, 214

Domänennamen
auswählen, 68
`/etc/defaultdomain`-Datei, 114, 255
Top-Level-Domain, 68
Drahtlose Kommunikation
Mobile IP, 726, 730, 741
Dreifach-Handshake, 47
DS Codepoint (DSCP), 833, 836
AF-Weiterleitung Codepoint, 837, 914
auf einem Diffserv-Router konfigurieren, 890, 914
`dscp_map`-Parameter, 915
EF-Weiterleitung Codepoint, 837, 914
Farberkennung konfigurieren, 912
in der IPQoS-Konfigurationsdatei definieren, 873
PHBs und der DSCP, 836
Planung, in der QoS-Richtlinie, 856
`dscpmk`-Marker, 833
in einer Marker `action`-Anweisung aufrufen, 873, 879, 885, 888
Paketweiterleitung planen, 856
PHBs zur Weiterleitung von Paketen, 913
DSS-Authentifizierungsalgorithmus, 662
Dual-Stack-Protokolle, 93, 283
Dynamic Host Configuration Protocol, *Siehe* DHCP-Protokoll
Dynamische Rekonfiguration (DR)
ausgefallene Schnittstellen ersetzen, 815-817
beim Systemstart fehlende NICs, 795-796
Definition, 783
DR-Attach-Verfahren, 817
DR-Detach-Verfahren, 816-817
Interoperation mit IPMP, 793-796
Schnittstelle ersetzen, die beim Systemstart nicht vorhanden war, 818-820
Schnittstellen von einer IPMP-Gruppe trennen, 794-795
Schnittstellen wieder bei einer IPMP-Gruppe anschließen, 795
Schnittstellen zu einer IPMP-Gruppe hinzufügen, 794
Dynamische Schnittstellen
Agent Advertisement-Nachrichten über, 730, 765
Dynamisches Routing, 141
Dynamisches Routing *(Fortsetzung)*
auf einem Host mit einer Schnittstelle konfigurieren, 140
Beispiel einer Hostkonfiguration, 142
Eignung für, 132

E

EGP, *Siehe* Routing-Protokolle
Einschalten
eines IPv6-konformen Netzwerks, 191-192
Netzwerkkonfigurationsdaemons, 112
Empfangender Host
Paketpfad durch, 48, 49
Encapsulating Security Payload (ESP)
Beschreibung, 521-522
IP-Pakete schützen, 513
IPsec-Schutzmechanismus, 520-524
Sicherheitsbetrachtungen, 522
`encr_algs`-Sicherheitsoption, `ifconfig`-Befehl, 601
`encr_auth_algs`-Sicherheitsoption, `ifconfig`-Befehl, 600-601
Erkennung doppelt vorhandener Adressen
Algorithmus, 303
DHCP-Service, 386
IPv6, 85
Ermittelung des nächsten Hop, IPv6, 85
Ersetzen
IPsec SAs, 546
manuelle Schlüssel (IPsec), 546
PresharedKeys (IKE), 616-617
Erstellen
DHCP-Makros, 426
DHCP-Optionen, 433
IPsec SAs, 537, 545-549
`ipsecinit.conf`-Datei, 536
Security Parameter Index (SPI), 544
selbst-signierte Zertifikate (IKE), 625
sicherheitsbezogene Rolle, 551-552
Standortspezifisches SMF-Manifest, 589-591
TCP/IP-Netzwerke
`in.ndpd`-Aktivität verfolgen, 236-237
`in.routed`-Aktivität verfolgen, 235-236
Zertifikat-Anforderungen, 631

Erzeugen, Zufallszahlen, 543-544
ESP, *Siehe* Encapsulating Security Payload (ESP)
/etc/bootparams-Datei, 269
/etc/default/dhcpagent-Datei, 465-466
/etc/default/dhcpagent-Datei, Beschreibung, 505
/etc/default/inet_type-Datei, 234-235
  DEFAULT_IP-Wert, 294
/etc/default/mpathd-Datei, 820
/etc/defaultdomain-Datei
  Beschreibung, 255
  für den Netzwerk-Clientmodus löschen, 114
  lokale Dateien-Modus konfigurieren, 111
/etc/defaultrouter-Datei
  Beschreibung, 255
  lokale Dateien-Modus konfigurieren, 111
/etc/dhcp/dhcptags-Datei
  Beschreibung, 506
  Einträge umwandeln, 506
/etc/dhcp/eventhook-Datei, 474
/etc/dhcp/inittab-Datei
  ändern, 439
  Beschreibung, 506
/etc/dhcp.*Schnittstelle*-Datei, 459, 465
/etc/dhcp.*Schnittstelle*-Datei, Beschreibung, 505
/etc/dhcp/*Schnittstelle*.dhc-Datei, Beschreibung, 505
/etc/ethers-Datei, 270
/etc/hostname.*interface*-Datei, Lokaler Dateimodus, 110
/etc/hostname.*Schnittstelle*-Datei
  Beschreibung, 254
/etc/hostname.*Schnittstelle*-Datei
  manuelle Konfiguration, 150, 160
/etc/hostname.*Schnittstelle*-Datei,
  Netzwerkclient-Modus konfigurieren, 114
/etc/hostname.*Schnittstelle*-Datei
  Routerkonfiguration, 128
/etc/hostname6.ip.6to4tun0-Datei, 208
/etc/hostname6.ip.tun-Datei, 206, 207
/etc/hostname6.Schnittstelle-Datei,
  IPv6-Tunneling, 309
/etc/hostname6.*Schnittstelle*-Datei, Schnittstellen manuell konfigurieren, 186-188
/etc/hostname6.*Schnittstelle*-Datei, Syntax, 288-289
/etc/hosts-Datei, *Siehe* /etc/inet/hosts-Datei
/etc/inet/dhcpsvc.conf-Datei, 357
/etc/inet/hosts-Datei, 536
  Format, 256
  Hostname, 257
  lokale Dateien-Modus konfigurieren, 110
  Loopback-Adresse, 257
  mehrere Netzwerkschnittstellen, 257
  Netzwerkclient-Modus konfigurieren, 114
  Teilnetze hinzufügen, 106
  ursprüngliche Datei, 256, 257
/etc/inet/ike/config-Datei
  Beispiel, 613
  Beschreibung, 606, 658
  cert_root-Schlüsselwort, 633, 639
  cert_trust-Schlüsselwort, 628, 638
  ignore_crls-Schlüsselwort, 634
  ikecert-Befehl und, 661
  ldap-list-Schlüsselwort, 642
  PKCS #11-Bibliothekseintrag, 660
  pkcs11_path-Schlüsselwort, 636, 660
  PresharedKeys, 614
  proxy-Schlüsselwort, 642
  PublicKey-Zertifikate, 633, 639
  selbst-signierte Zertifikate, 628
  Sicherheitsbetrachtungen, 659
  Übertragungsparameter, 655
  use_http-Schlüsselwort, 642
  Zertifikate auf Hardware ablegen, 638
  Zusammenfassung, 609
/etc/inet/ike/crls-Verzeichnis, 664
/etc/inet/ike/publickeys Verzeichnis, 663
/etc/inet/ipaddrsel.conf-Datei, 243, 289
/etc/inet/ipnodes-Datei, 259, 536
/etc/inet/ipsecinit.conf-Datei, 595-596
/etc/inet/ndpd.conf-Datei, 194, 296
  6to4-Advertisement-Nachrichten, 278
  6to4-Router Advertisement-Nachrichten, 210
  erstellen·, 194
  Schlüsselwörter, 284-288, 296
  temporäre Adressen konfigurieren, 198
  Variablen zur Präfixkonfiguration, 286
  Variablen zur Schnittstellenkonfiguration, 285
/etc/inet/netmasks-Datei
  bearbeiten, 262, 263

/etc/inet/netmasks-Datei *(Fortsetzung)*
Routerkonfiguration, 129
Teilnetze hinzufügen, 106
/etc/inet/networks-Datei, Übersicht, 271
/etc/inet/protocols-Datei, 272
/etc/inet/secret/ike.privatekeys-Verzeichnis, 663
/etc/inet/services-Datei, Beispiel, 272
/etc/ipf/ipf.conf-Datei, *Siehe* Oracle Solaris IP Filter
/etc/ipf/ipnat.conf-Datei, *Siehe* Oracle Solaris IP Filter
/etc/ipf/ippool.conf-Datei, *Siehe* Oracle Solaris IP Filter
/etc/ipnodes-Datei entfernt, 511-513
/etc/netmasks-Datei, 263
/etc/nodename-Datei
Beschreibung, 255
für den Netzwerkclient-Modus löschen, 114
/etc/nsswitch.conf-Datei, 267, 269
ändern, 268, 269
Änderungen, zur IPv6-Unterstützung, 316-317
Beispiele, 268
Namen-Service-Vorlagen, 268
Netzwerkclient-Modus konfigurieren, 114
Syntax, 268
von DHCP verwendet, 505
/etc/resolv.conf-Datei, von DHCP verwendet, 505
Ethernet-Adressen
Siehe ethers-Datenbank
Siehe MAC-Adresse
ethers-Datenbank
Einträge überprüfen, 248
entsprechende Namen-Service-Dateien, 266
Übersicht, 270
eventhook-Datei, 474
Expedited Forwarding (EF), 837, 914
in der IPQoS-Konfigurationsdatei definieren, 874
expire_timer-Schlüsselwort, IKE-Konfigurationsdateifile, 655

F

-F-Option, ikecert certlocal-Befehl, 626
-f-Option
in.iked-Daemon, 615
ipseckey-Befehl, 539
Failback
Definition, 782-783
dynamische Rekonfiguration (DR) mit, 795
Failover
Beispiele, 791
Definition, 782
dynamische Rekonfiguration (DR) und, 794-795
Standby-Schnittstelle, 788
failover-Option, ifconfig-Befehl, 785
Failure Detection Time, IPMP, 790
Farberkennung, 833, 911
Fehlerbehebung
DHCP, 477
IKE-Nutzlast, 636
IKE-Übertragungstiming, 654-656
IPv6-Probleme, 249-251
PPP-Links prüfen
Paketfluss, 238
TCP/IP-Netzwerke
allgemeine Methoden, 247, 248
Diagnoseprogramme von Drittanbietern, 247
Netzwerkstatus mit dem netstat-Befehl überwachen, 225
Pakete zwischen Client und Server prüfen, 241
Paketübertragung mit dem Befehl snoop überwachen, 238
Paketverlust, 233
ping-Befehl, 233
Remote-Hosts mit dem Befehl ping sondieren, 232
Schnittstellenstatus mit dem Befehl ifconfig anzeigen, 221, 224
Softwareprüfungen, 248
Statistiken nach Protokoll beziehen, 226-227
Status bekannter Routen anzeigen, 231-232
traceroute-Befehl, 237-238
Transportprotokollstatus beziehen, 227-228
Übertragungen von Schnittstellen abrufen, 228-229
Fehlermeldungen für IPQoS, 897
Filter, 832

Filter *(Fortsetzung)*
- erstellen, in der IPQoS-Konfigurationsdatei, 878, 883
- `filter`-Klausel, Syntax, 923
- Planung, in der QoS-Richtlinie, 850

`filter`-Klausel, in der IPQoS-Konfigurationsdatei, 871, 923

filters, Liste der Selektoren, 908

Flow Accounting, 902, 917
- Flow-Tabelle, Datensätze, 918

`flowacct`-Modul, 834, 917
- `acctadm`-Befehl, zum Erstellen einer Flow Accounting-Datei, 920
- `action`-Anweisung für `flowacct`, 876
- Attribute von Flow-Datensätzen, 919
- Flow-Datensätze, 902
- Flow-Tabelle, Datensätze, 918
- Parameter, 918

Foreign-Agent
- Agent, 725
- arbeiten ohne, 731
- Authentifizierung, 751
- bei mehreren registrieren, 734
- Besucherliste, 756, 774
- Care-Of-Adresse, 730, 734, 739
- Definition, 726
- durch Verwenden registrieren, 733, 734
- Implementierung, 759
- Leistungsumfang festlegen, 744
- mobile Knoten bedienen, 729
- Nachrichtenauthentifizierung, 770, 771
- Registrierungsanforderung weiterleiten, 736
- Registrierungsnachricht, 728
- Service anfordern von, 737
- Überlegungen, 737
- Unterstützung der Kapselung, 738
- Unterstützung der Sicherheitszuordnung, 736

Foreign-Netzwerk, 726, 733, 739

`ForeignAgent`-Label, 746, 755, 765

Fragmentierte Pakete, 41

Framing
- Beschreibung, 48
- Sicherungsschicht, 40, 48

`ftp` Programm, 43

`ftp` Programm *(Fortsetzung)*
- Anonymes FTP, Programm
  - Beschreibung, 43

G

Gateway, in einer Netzwerktopologie, 131

Gekapseltes Datagramm, Mobile IP, 726

`General`-Abschnitt
- Mobile -Konfigurationsdatei, 765
- `Version`-Label, 765

`gethostbyname`-Befehl, 317

`getipnodebyname`-Befehl, 317

Getrennte dezimale Notation, 61

Globale Zone, IKE, 603

`GlobalSecurityParameters`-Abschnitt
- Label und Werte, 767
- Mobile IP-Konfigurationsdatei, 767-768

Grenzrouter, 124

Grenzrouter, an einem 6to4-Standort, 313

`group`-Parameter
- `ifconfig`-Befehl, 802, 815

H

`HA-FAauth`-Label, 746, 751, 767

Handshake, dreifach, 47

Hardware
- Beschleunigen von IKE-Berechnungen, 651
- Bitübertragungsschicht (OSI), 39
- Bitübertragungsschicht (TCP/IP), 39, 40
- IKE-Berechnungen beschleunigen, 608
- IKE-Schlüssel speichern, 608, 652-654

Hardware für IPQoS-konforme Netzwerke, 842

Header der Pakete, IP-Header, 48

Header-Felder, IPv6, 281

Hinzufügen
- CA-Zertifikate (IKE), 631-636
- IPsec SAs, 537, 545-549
- PresharedKeys (IKE), 619-622
- PublicKey-Zertifikate (IKE), 631-636
- Schlüssel manuell (IPsec), 545-549
- selbst-signierte Zertifikate (IKE), 625

Home-Adresse, 724, 725, 726
Home-Agent
  Address-Abschnitt, 770, 771
  Antwort auf Registrierungsanforderung, 737
  Authentifizierung, 751
  Bindungstabelle, 756, 757, 774
  Datagramme weiterleiten, 739
  Datagrammzustellung, 725
  dynamische Adresszuweisung, 768
  dynamische Erkennung, 738
  Implementierung, 759
  Kapselung, 738
  Leistungsumfang festlegen, 744
  Registrierung aufheben, 734
  Registrierungsanforderung, 736, 737
  Registrierungsnachricht, 728, 734
home agent, Replay-Schutz, 767
Home-Agent
  Standort des mobilen Knoten, 728
  Statusinformationen, 775
  Überlegungen, 737
  Unterstützung der Sicherheitszuordnung, 736
Home-Foreign-Agent-Authentifizierung, 736
Home-Netzwerk, 725, 726, 734, 737
HomeAgent-Label, 746, 755, 765
-Hop (Paketweiterleitung), 119
Hops, Relay-Agent, 386
Host
  6to4-Adresse konfigurieren, 279
  empfangender
    Paketpfad durch, 48
Host-Konfigurationsmodi (TCP/IP), 103, 106
  Beispielnetzwerk, 105
  gemischte Konfigurationen, 105
  IPv4-Netzwerktopologie, 106
  lokale Dateien-Modus, 104, 105
  Netzwerkclient-Modus, 105
  Netzwerkkonfigurationsserver, 104
Host zu Host-Kommunikation, 40
hostconfig-Programm, 114
Hostname, Client zur Anforderung eines bestimmten Hostnamen konfigurieren, 468
hostname.*Schnittstelle*-Datei
  Beschreibung, 254
hostname.*Schnittstelle*-Datei, in IPMP, 809
hostname.*Schnittstelle*-Datei
  Routerkonfiguration, 128
hostname6.ip.tun-Datei, 206, 207
hostname6.*Schnittstelle*-Datei, Schnittstellen manuell konfigurieren, 186-188
hostname6.*Schnittstelle*-Datei, Syntax, 288-289
Hosts
  Beispielnetzwerk, 105
  empfangender
    Paketpfad durch, 49
  Fehlersuche bei allgemeinen Problemen, 247
  für IPv6 konfigurieren, 196-204
  Host-Konnektivität prüfen mit ping, 232
hosts
  Hostname
    /etc/inet/hosts-Datei, 257
Hosts
  Hostname
    Verwaltung, 66
  in einer IPv4-Netzwerktopologie, 106
  in einer IPv4-Routing-Topologie, 125
  IP-Konnektivität prüfen, 233
  Multihomed
    Definition, 125
    Konfiguration, 134
  Routing-Protokoll auswählen, 129
  sendender
    Paketpfad durch, 46, 48
  TCP/IP-Konfigurationsmodi, 106
    Beispielnetzwerk, 105
    gemischte Konfigurationen, 105
    Konfigurationsinformationen, 103
    lokale Dateien-Modus, 104, 105, 112
    Netzwerkclient-Modus, 105, 114
    Netzwerkkonfigurationsserver, 104
  temporäre IPv6-Adressen, 196-199
hosts.byaddr-Map, 214-215
hosts.byname-Map, 214-215
hosts-Datei, 536
hosts-Datenbank, 255, 258
  Auswirkungen des Namen-Services, 258
  Einträge überprüfen, 248
  entsprechende Namen-Service-Dateien, 266

hosts-Datenbank *(Fortsetzung)*
/etc/inet/hosts-Datei
Format, 256
Hostname, 257
lokale Dateien-Modus konfigurieren, 110
Loopback-Adresse, 257
mehrere Netzwerkschnittstellen, 257
Netzwerkclient-Modus konfigurieren, 114
Routerkonfiguration, 128
Teilnetze hinzufügen, 106
ursprüngliche Datei, 256, 257
Namen-Service
Auswirkungen, 258
Namen-Services
Formen von, 265
hosts.org_dir-Tabelle, 214-215
http-Zugriff auf CRLs, use_http-Schlüsselwort, 642

I

ICMP-Protokoll
aufrufen, mit ping, 232
Beschreibung, 41
Nachrichten, im Neighbor Discovery-Protokoll, 299-300
Statistiken anzeigen, 226
ICMP Router Discovery (RDISC)-Protokoll, 274
Identity Association, 456
ifconfig-Befehl, 309, 670
6to4-Erweiterungen, 209
als Tool zur Fehlersuche verwenden, 247
Anzeigen des Schnittstellenstatus, 221
Ausgabeformat, 222
auth_algs-Sicherheitsoption, 600
deprecated-Attribut, 786
DHCP-Client steuern, 464
DHCP und, 498
encr_algs-Sicherheitsoption, 601
encr_auth_algs-Sicherheitsoption, 600-601
failover-Option, 785
group-Parameter, 802, 815
Informationen in der Ausgabe, 222
IPMP-Erweiterungen für, 780
IPMP-Gruppe anzeigen, 812
ifconfig-Befehl *(Fortsetzung)*
IPsec-Sicherheitsoptionen, 599-601
IPv6-Erweiterungen für, 292
Konfiguration
IPv-Tunnel, 293
VLAN-Geräte, 154
Plumben einer Schnittstelle, 127, 149, 159
Reihenfolge der STREAMS-Module überprüfen, 800
Schnittstelle plumben (aktivieren), 166
Schnittstellenstatus anzeigen, 224, 788
standby-Parameter, 787, 809
Syntax, 221
test-Parameter, 802
ignore_crls-Schlüsselwort, IKE-Konfigurationsdatei, 634
IGP, *Siehe* Routing-Protokolle
IKE
&sca-Board verwenden, 661, 662
Ändern
Privilegstufe, 618, 660
angehängte Hardware suchen, 650
Anzeigen
PresharedKeys, 618-619
Befehlsbeschreibungen, 608-610
crls-Datenbank, 664
Daemon, 658
Datenbanken, 660-664
Fehlerbehebung beim Übertragungstiming, 654-656
Globale Zone, 603
Hardware-Speicherung von Schlüsseln, 608
Hardwarebeschleunigung, 608
ike.preshared-Datei, 660
ike.privatekeys-Datenbank, 663
ikeadm-Befehl, 659-660
ikecert-Befehl, 660
ikecert certdb-Befehl, 632
ikecert certrldb-Befehl, 642
ikecert tokens-Befehl, 653
Implementierung, 611
in.iked-Daemon, 658
ISAKMP SAs, 605

IKE *(Fortsetzung)*
- Konfiguration
  - für mobile Systeme, 643-650
  - mit CA-Zertifikaten, 631-636
  - mit PresharedKeys, 612
  - mit PublicKey-Zertifikaten, 624
- Konfigurationsdateien, 608-610
- mobile Systeme und, 643-650
- NAT und, 647-648, 649
- Perfect Forward Secrecy (PFS), 604
- Phase 1 Exchange, 605
- Phase 1 Schlüsselaushandlung, 654-656
- Phase 2 Exchange, 606
- PKCS #11-Bibliothek, 662
- PresharedKeys, 606
  - Anzeigen, 618-619
- Privilegstufe
  - Ändern, 618, 660
  - Beschreibung, 659
  - Prüfen, 618
  - überprüfen, 617
- `publickeys` Datenbank, 663
- Referenz, 657
- RFCs, 514
- Richtlinie auf Gültigkeit prüfen, 615
- Schlüsselmanagement, 604
- selbst-signierte Zertifikate erstellen, 625
- selbst-signierte Zertifikate hinzufügen, 625
- Sicherheitszuordnungen, 658
- SMF-Service, 657-658
- SMF-Servicebeschreibung, 608-610
- Speicherorte für Schlüssel, 608-610
- Sun Crypto Accelerator 1000-Board verwenden, 651-652
- Sun Crypto Accelerator 4000-Board verwenden, 652-654
- Sun Crypto Accelerator 6000-Board verwenden, 652-654
- Sun Crypto Accelerator-Board verwenden, 663
- Übersicht, 604
- UltraSPARC T2-Prozessor verwenden, 651
- Verwalten mithilfe von SMF, 553-554
- Zertifikat-Anforderungen erzeugen, 631
- Zertifikate, 607

`ike/config`-Datei, *Siehe* `/etc/inet/ike/config`-Datei
`ike.preshared`-Datei, 615, 660
`ike.preshared` Datei, Beispiel, 621
`ike.privatekeys`-Datenbank, 663
`ike`-Service
- Beschreibung, 520, 594
- Verwenden, 537

`ikeadm`-Befehl
- Beschreibung, 658, 659-660
- Privilegstufe
  - Prüfen, 618
  - überprüfen, 617

`ikecert`-Befehl
- `-A`-Option, 662
- `-a`-Option, 637
- Beschreibung, 658, 660
- `-T`-Option, 637, 662
- `-t`-Option, 662

`ikecert certdb`-Befehl
- `-a`-Option, 627, 632

`ikecert certlocal`-Befehl
- `-kc`-Option, 631
- `-ks`-Option, 625

`ikecert certrldb`-Befehl, `-a`-Option, 642
`ikecert tokens`-Befehl, 653
`in.dhcpd`-Daemon, 330
- Beschreibung, 498
- Debugging-Modus, 485

`in.iked`-Daemon
- aktivieren, 658
- Beschreibung, 604
- `-c`-Option, 615
- `-f`-Option, 615
- Privilegstufe
  - Prüfen, 618
  - überprüfen, 617
- stoppen und starten, 539, 617

`in.mpathd`-Daemon
- Definition, 780-781
- Stichprobenrate, 780
- Stichprobenziele, 790

`in.ndpd`-Daemon
- Optionen, 296
- Protokoll erstellen, 236-237

in.ndpd-Daemon *(Fortsetzung)*
Status prüfen, 249
in.rarpd-Daemon, 104
in.rdisc-Programm, Beschreibung, 274
in.ripngd-Daemon, 193, 297
in.routed-Daemon, 141
Beschreibung, 273
Platz sparender Modus, 273
Protokoll erstellen, 235-236
in.telnet Daemon, 43
in.tftpd-Daemon
Beschreibung, 104
einschalten, 112
Inaktive Regelliste, *Siehe* Oracle Solaris IP Filter
inet_type-Datei, 234-235
inetd-Daemon
IPv6-Services und, 297-299
Services verwalten, 263
inetd-Daemon, Status prüfen, 248
inetd-Daemon
vom Daemon gestartete Services, 142
Interaktiver Modus, ipseckey-Befehl, 546
Internet, Domain-Namen-Registrierung, 38
Internet Assigned Numbers Authority (IANA), Registrierungsservices, 63
Internet Drafts
Definition, 50
SCTP mit IPsec, 514
Internet Protocol (IP), 724
Internet Security Association and Key Management Protocol (ISAKMP) SAs, Beschreibung, 605
Internet Security Association und Key Management Protocol (ISAKMP) SAs, Speicherort, 660
Internetschicht
Paket-Lebenszyklus
sendender Host, 48
Internetzwerke
Definition, 69
Paketübertragung per Router, 71, 72
Redundanz und Zuverlässigkeit, 70
Topologie, 69, 70
InterNIC
Registrierungsservices
Domain-Namen-Registrierung, 38
Interoperabilität
IPsec mit anderen Plattformen bei Verwendung von PresharedKeys, 616
IPsec mit anderen Plattformen im Tunnelmodus, 512
IP-Addressen
DHCP
Eigenschaften ändern, 410
IP-Adresse
BaseAddress-Label, 768
Care-Of-Adresse, 730
IP-Quelladresse, 739, 740
mobiler Knoten, 726, 736
IP-Adressen
Adressen aller Schnittstellen anzeigen, 224
Adressierungsschema entwerfen, 58, 66
DHCP
Aufgaben, 402
Eigenschaften, 403
Fehler, 481
für Client reservieren, 416
hinzufügen, 406
löschen, 413
nicht verwendbar, 413
Funktionen des IP-Protokolls, 40
mit DHCP zuordnen, 346
Netzwerkklassen
Netzwerknummern verwalten, 58
Netzwerkschnittstellen und, 65
Probleme mit Teilnetzen, 262
IP-Datagramme
Formatierung im IP-Protokoll, 40
Funktionen des UDP-Protokolls, 42
IP-Header, 48
mit IPsec schützen, 513
Paketprozess, 48
IP Filter, *Siehe* Oracle Solaris IP Filter
IP-Link, in IPMP-Terminologie, 781
IP Network Multipathing (IPMP), *Siehe* IPMP
IP-Protokoll
Beschreibung, 40
Host-Konnektivität prüfen, 232, 233
Statistiken anzeigen, 226
IP Security Architecture, *Siehe* IPsec

ip_strict_dst_multihoming, Verhindern von IP-Spoofing, 589-591
IP-Weiterleitung
  in IPv4-VPNs, 560, 563, 577, 579
  in IPv6 VPNs, 571, 575, 584
  in VPNs, 527
  IPv4-VPNs, 565
  IPv6-VPNs, 573, 586, 587
ipaddrsel Befehl, 243
ipaddrsel-Befehl, 289-290
ipaddrsel.conf-Datei, 243, 289
ipf-Befehl
  Siehe auch Oracle Solaris IP Filter
  -6-Option, 678-679
  -a-Option, 697-699
  -D-Option, 687
  -E-Option, 683-684
  -F-Option, 686, 699, 702
  -f-Option, 683-684, 697-699, 699-700, 700-701
  -I-Option, 700-701, 702
  Regeln über Befehlszeile hinzufügen, 699-700
  -s-Option, 701-702
ipf.conf-Datei, 671-674
  Siehe Oracle Solaris IP Filter
ipfstat-Befehl, 707-708
  Siehe auch Oracle Solaris IP Filter
  -6-Option, 678-679
  -i-Option, 696-697, 697
  -o-Option, 696-697, 697
  -s-Option, 708-709
  -t-Option, 707-708
ipgpc-Classifier, *Siehe* Classifier-Modul
ipmon-Befehl
  Siehe auch Oracle Solaris IP Filter
  -a-Option, 711-713
  -F-Option, 713
  IPv6 und, 678-679
  -o-Option, 711-713
IPMP
  allgemeine Anforderungen, 783-784
  ATM-Unterstützung, 801
  Ausfallerkennung
    Definition, 782
  Datenadressen, 784

IPMP *(Fortsetzung)*
  Dynamische Rekonfiguration, 783, 793-796
  Ethernet-Unterstützung, 801
  Failover
    Definition, 782
  Failure Detection Time, 790
  -Gruppe, Konfiguration
    Aufgaben bei der Konfiguration, 801-806
    Fehlerbehebung, 805
    für eine IPMP-Gruppe planen, 799-801
  hostname.*Schnittstelle*-Datei, 809
  IP-Links, Typen, 781
  IPMP-Konfigurationsdatei, 820-822
  Konfiguration nach Neustart beibehalten, 804, 805, 809
  Lastverteilung, 780
  Multipathing-Gruppe, Definition
    Siehe IPMP-Gruppe
  Reparaturerkennung, 782-783
  Schnittstelle ersetzen, die beim Systemstart nicht vorhanden war, 818-820
  Schnittstellen ersetzen, DR, 815-817
  Schnittstellenkonfiguration
    aktiv-aktiv, 788
  -Schnittstellenkonfiguration
    Aktiv-Standby, 788
    Arten von Schnittstellenkonfigurationen, 787
    Standby-Schnittstelle, 787-788
  Schnittstellenkonfiguration
    Standby-Schnittstelle, 808-810
  Softwarekomponenten, 780
  Stichproben-basierte Ausfallerkennung, 789, 790-791
  Stichprobenverkehr, 784
  Terminologie, 781-783
  Testadressen, 784-786
  Token Ring-Unterstützung, 801
  Übersicht, 779-783
  unterstützte Netzwerktreiber, 789
  Verwaltung, 812-815
  Zielsysteme, 783
    in einem Skript konfigurieren, 807-808
    manuell konfigurieren, 807
IPMP-Daemonin.mpathd, 780-781

IPMP-Gruppe, Ausfall einer Gruppe, 791
IPMP-Gruppen
  Auswirkungen von Schnittstellen, die bei einem Neustart nicht vorhanden sind, 795-796
  eine Gruppe für eine einzelne Schnittstelle konfigurieren, 810-812
  Fehler bei der Gruppenkonfiguration beheben, 805
  Gruppenmitgliedschaft anzeigen, 812-813
  konfigurieren, 801-806
  NIC-Geschwindigkeit in einer Gruppe, 782
  Planungsaufgaben, 799-801
  Schnittstelle aus einer Gruppe entfernen, 814-815
  Schnittstelle zu einer Gruppe hinzufügen, 813
  Schnittstelle zwischen Gruppen verschieben, 815
  Schnittstellen entfernen, über DR, 794-795
  Schnittstellen hinzufügen, über DR, 794
  Schnittstellen wieder anschließen, über DR, 795
`ipnat`-Befehl
  Siehe auch Oracle Solaris IP Filter
  `-C`-Option, 687
  `-F`-Option, 687, 703-704
  `-f`-Befehl, 704
  `-f`-Option, 683-684
  `-l`-Option, 703
  Regeln über die Befehlszeile anhängen, 704
  `-s`-Option, 709
`ipnat.conf`-Datei, 674-675
  Siehe Oracle Solaris IP Filter
`ipnodes.byaddr`-Map, 214-215
`ipnodes.byname`-Map, 214-215
`ipnodes`-Datei, 259, 536
`ipnodes.org_dir`-Tabelle, 214-215
`ippool`-Befehl
  Siehe auch Oracle Solaris IP Filter
  `-F`-Option, 705-706
  `-f`-Option, 706
  IPv6 und, 678-679
  `-l`-Option, 705
  Regeln über die Befehlszeile anhängen, 706
  `-s`-Option, 709-710
`ippool.conf`-Datei, 675-677
  Siehe Oracle Solaris IP Filter
IPQoS, 825
  Fehlermeldungen, 897

IPQoS *(Fortsetzung)*
  Funktionen, 826
  Funktionen zur Verwaltung von Datenverkehr, 829, 831
  Konfigurationen planen, 841
  Konfigurationsbeispiel, 859-861
  Konfigurationsdatei, 865, 920
    `action`-Anweisung, Syntax, 922
    `class`-Klausel, 869
    erste `action`-Anweisung, 921
    erste action-Anweisung, 868
    `filter`-Klausel, 871
    Liste der IPQoS-Module, 922
    Marker `action`-Anweisung, 873
    Syntax, 921
  Manpages, 827
  Nachrichtenprotokollierung, 896
  Netzwerkbeispiel, 865
  QoS-Richtlinie planen, 845
  Richtlinien für IPv6-konforme Netzwerke, 96
  Router in einem IPQoS-Netzwerk, 890
  sachverwandte RFCs, 827
  Statistiken erzeugen, 904
  Umsetzung des Diffserv-Modells, 831
  unterstützte Netzwerktopologien, 842, 843, 844
  Unterstützung von VLAN-Geräten, 915
IPQoS-Konfigurationsdateien, Beispiel
  Anwendungsserver, 880
  Beste Leistung-Webserver, 867
  Premium-Webserver, 866
  Segment zur Erkennung von Farben, 911
  VLAN-Gerät konfigurieren, 916
`ipqosconf`, 865
`ipqosconf`-Befehl
  aktuelle Konfiguration auflisten, 895
  Befehlsoptionen, 924
  eine Konfiguration übernehmen, 894, 896
IPsec
  Ablauf bei abgehenden Paketen, 516
  Ablauf bei eingehenden Paketen, 516
  aktivieren, 530
  Algorithmusquelle, 597
  angeben
    Authentifizierungsalgorithmen, 600

IPsec, angeben *(Fortsetzung)*
Verschlüsselungsalgorithmen, 600
Authentifizierungsalgorithmen, 523
-Befehle, Liste, 530-532
Daten einkapseln, 521
Datenverkehr sichern, 535-539
Einstellen der Richtlinie
Vorübergehend, 594-595
Encapsulating Security Payload (ESP), 520-524
Erweiterungen für Dienstprogramme
`ifconfig`-Befehl, 599-601
`snoop`-Befehl, 599, 601
`/etc/hostname.ip6.tun0`-Datei
Konfigurieren des VPN, 573, 585
`/etc/hosts`-Datei, 536
`/etc/inet/ipnodes`-Datei, 536
`hostname.ip.tun0`-Datei
Konfigurieren des VPN, 579
`ifconfig`-Befehl
Konfigurieren des VPN, 564
Konfigurieren eines VPN, 574, 586
Sicherheitsoptionen, 599-601
Implementierung, 533
`in.iked`-Daemon, 520
Interoperabilität mit anderen Plattformen
IP-in-IP-Tunneln, 512
Preshared Schlüssel, 543, 616
`ipsecalgs`-Befehl, 523, 597
`ipsecconf`-Befehl, 524, 594-595
`ipsecinit.conf`-Datei
Beschreibung, 595-596
IPsec-Umgebung eines LAN löschen, 569, 582
konfigurieren, 536
LAN umgehen, 600
Richtliniendatei, 524
Schützen des Webservers, 540, 541
Umgehen des LAN, 562, 578
`ipseckey`-Befehl, 520, 598-599
IPv4 VPN im Transportmodus, und, 576-583
IPv4 VPNs, und, 560-570
IPv6 VPN im Transportmodus, und, 583-589
IPv6 VPNs, und, 570-576
Komponenten, 513
Konfigurationsdateien, 530-532

IPsec *(Fortsetzung)*
konfigurieren, 524
Konfigurieren, 594-595
logische Domänen und, 530
NAT und, 528-529
Paketschutz überprüfen, 550-551
RBAC und, 535
RFCs, 514
Richtlinie einrichten
permanent, 595-596
Richtlinien anzeigen, 542-543
Richtlinienbefehl
`ipsecconf`, 594-595
Richtliniendateien, 595-596
`route`-Befehl, 564, 566, 574, 575, 580, 581, 586, 587
SAs manuell erstellen, 545-549
Schlüssel-Dienstprogramme
IKE, 604
`ipseckey`-Befehl, 598-599
Schlüsselmanagement, 519-520
schützen
mobile Systeme, 643-650
Pakete, 513
VPNs, 560-570
Webserver, 539-542
Schutzmechanismen, 520-524
Schutzrichtlinie, 524
SCTP-Protokoll und, 529, 535
Security Parameter Index (SPI), 519-520
Security Policy Database (SPD), 594
Security Policy-Datenbank (SPD), 513, 515
Services
`ipsecalgs`, 531
`manueller Schlüssel`, 531
`Richtlinie`, 530
-Services, Liste, 530-532
Services aus SMF, 511-513, 593-594
Sichere Remoteanmeldung, 536
Sicherheitsmechanismen, 513
Sicherheitsprotokolle, 513, 519-520
Sicherheitsrollen, 551-552
Sicherheitszuordnung-Datenbank (SADB), 513, 597
Sicherheitszuordnungen (SAs), 519-520

IPsec *(Fortsetzung)*
Sicherheitszuordnungen (SAs) ersetzen, 546
Sicherheitszuordnungen (SAs) hinzufügen, 537
snoop-Befehl, 599, 601
Solaris Cryptographic Framework und, 597
Terminologie, 515
Transportmodus, 525-527
Tunnel, 527
Tunnelmodus, 525-527
Übersicht, 513
umgehen, 524, 541
Umgehen, 540
Verschlüsselungsalgorithmen, 523
Verwalten mithilfe von SMF, 553-554
Verwenden von ssh für die sichere Remoteanmeldung, 538
Virtual Private Networks (VPNs), 560-570
virtuelle private Netzwerke (VPNs), 527
VPN schützen, 554-556, 557-591
Zonen und, 529, 535
Zufallszahlen für Schlüssel erzeugen, 543-544
IPsec-Richtlinie
Angeben, 572, 585
Beispiel von Tunneln im Transportmodus, 582
Beispiel zur Verwendung einer eingestellten Syntax, 582-583
Beispiele für eine Tunnelsyntax, 555-556
IP-in-IP-Datagramme, 511-513
LAN-Beispiel, 569
IPsec-Tunnel, Vereinfachte Syntax, 511-513
ipsecalgs-Service, Beschreibung, 593
ipsecconf-Befehl
-a-Option, 539
Beschreibung, 531
-f-Option, 539
IPsec-Richtlinie anzeigen, 539-542, 542-543, 595-596
Konfigurieren der IPsec-Richtlinie, 594-595
Sicherheitsbetrachtungen, 539, 596
Zweck, 524
ipsecconfBefehl, Definieren von Tunneln, 525
ipsecinit.conf-Datei
Beispiel, 595
Beschreibung, 530
ipsecinit.conf-Datei *(Fortsetzung)*
IPsec-Umgebung eines LAN löschen, 569, 582
Schützen des Webservers, 540, 541
Sicherheitsbetrachtungen, 596
Speicherort und Geltungsbereich, 529
Tunneloptionen konfigurieren, 600
Überprüfen der Syntax, 537
Umgehen des LAN, 562, 578
Zweck, 524
ipseckey-Befehl
Beschreibung, 531, 598-599
Interaktiver Modus, 546
Sicherheitsbetrachtungen, 598-599
Zweck, 520
ipseckeys-Datei, IPsec-Schlüssel speichern, 531
IPv4 -Adressen, Teilnetznummer, 63
IPv4-Adresseen
Netzwerkklassen
Adressierungsschema, 62
IPv4-Adressen
Bereich der verfügbaren Zahlen, 63
Format, 61
getrennte dezimale Notation, 61
IANA-Zuweisung von Netzwerknummern, 63
Komponenten, 63
Netzmasken anwenden, 262
Netzwerkklassen, 63
Adressierungsschema, 63
Klasse A, 274
Klasse B, 275
Klasse C, 275
Probleme mit Teilnetzen, 260
symbolische Namen für Netzwerknummern, 263
IPv6
6to4-Adresse, 278
Adressierungsplan, 99
allgemeine IPv6-Probleme beheben, 249-251
ATM-Unterstützung, 318
auf einem Server aktivieren, 202-204
automatische Adresskonfiguration, 296, 300
automatische Tunnel, 309
bekannte Probleme bei einem 6to4-Router, 251
DNS AAAA-Datensätze, 215
DNS-Unterstützung vorbereiten, 96

IPv6 *(Fortsetzung)*
- doppelt vorhandene Adressen erkennen, 85
- Dual-Stack-Protokolle, 93
- Ermittelung des nächsten Hop, 85
- Erweiterungen für den Befehl `ifconfig`, 292
- Felder im Extension-Header, 282
- hinzufügen
  - Adressen zum NIS, 214-215
  - DNS-Unterstützung, 214
- im Vergleich mit IPv4, 304-306
- im Vergleich zu IPv4, 74
- `in.ndpd`-Daemon, 296
- `in.ripngd`-Daemon, 297
- Link-lokale Adressen, 302, 305
- Multicast-Adressen, 280-281, 305
- Neighbor Discovery-Protokoll, 299-306
- Neighbor Solicitation, 300
- Neighbor Solicitation und Unerreichbarkeit, 302
- Neighbor-Unerreichbarkeitserkennung, 85
- Neighbor Unreachability Detection, 305
- `nslookup`-Befehl, 216
- Paket-Header-Format, 281-282
- Protokollübersicht, 300
- Redirect, 300, 305
- Richtlinientabelle zur Standard-Adressenauswahl, 289
- Router Advertisement-Nachrichten, 299, 301, 304, 307
- Router-Erkennung, 296, 304
- Router Solicitation, 299, 301
- Routing, 306
- Sicherheitsbetrachtungen, 97-98
- Standort-lokale Adressen, 87
- Status von `in.ndpd` prüfen, 249
- statusfreie automatische Adresskonfiguration, 301, 302
- Teilnetze, 78
- temporäre Adresskonfiguration, 196-199
- Tunnel, 309-311
- Tunnel konfigurieren, 205-206
- Umleitung, 85
- und Oracle Solaris IP Filter, 678-679
- Verkehr überwachen, 241-242

IPv6-Adressen
- Adressauflösung, 85
- Anycast, 84
- automatische Adresskonfiguration, 85, 86-87
- Einmaligkeit, 302
- Link-lokal, 83
- Multicast, 83-84
- Schnittstellen-ID, 82
- Unicast, 81-82
- VPN-Verwendungsbeispiel mit IPsec, 570-576

IPv6-Leistungsmerkmale, Neighbor Discovery-Protokoll, 84

K

`-kc`-Option
- `ikecert certlocal`-Befehl, 625, 631, 661

`-ks`-Option
- `ikecert certlocal`-Befehl, 625, 661

Kapselungarten, Mobile IP, 738

`Key`-Label, 747, 752, 769

`KeyDistribution`-Label, 746, 768

Klasse A-Netzwerknummern
- Beschreibung, 274
- IPv4-Adressraum aufteilen, 63

Klasse B-Netzwerknummern
- Beschreibung, 275
- IPv4-Adressraum aufteilen, 63

Klasse C-Netzwerknummern
- Beschreibung, 275
- IPv4-Adressraum aufteilen, 63

Klassen, 832
- in der IPQoS-Konfigurationsdatei definieren, 877, 882
- Syntax der `class`-Klausel, 923

Knoten, IPv6, 77

Knotennamen
- lokaler Host, 114, 255

Konfiguration
- Adresspools, 675-677
- DHCP-Client, 453
- DHCP-Service, 355
- IKE, 611
- `ike/config`-Datei, 658

Konfiguration *(Fortsetzung)*
IKE mit CA-Zertifikaten, 631-636
IKE mit mobilen Systemen, 643-650
IKE mit PublicKey-Zertifikaten, 624, 625-630
IKE mit selbst-resignierten Zertifikaten, 625-630
IKE mit Zertifikaten auf Hardware, 636-640
IPsec im LAN, 569, 582
ipsecinit.conf-Datei, 595-596
IPv6-Routers, 192
NAT-Regeln, 674-675
Netzwerksicherheit mit einer Rolle, 551-552
Paketfilterung, Regeln, 671-674
Router, 273
Netzwerkschnittstellen, 126, 129
Übersicht, 126
TCP/IP-Konfigurationsdateien, 253
/etc/defaultdomain-Datei, 255
/etc/defaultrouter-Datei, 255
/etc/hostname. Schnittstelle-Datei, 254
/etc/nodename-Datei, 114, 255
hosts-Datenbank, 255, 258
netmasks-Datenbank, 260
TCP/IP-Konfigurationsmodi
Beispielnetzwerk, 105
gemischte Konfigurationen, 105
lokale Dateien-Modus, 104, 112
Netzwerkclient-Modus, 114
TCP/IP-Netzwerke
Konfigurationsdateien, 253
lokale Dateien-Modus, 112
Netzwerkclients, 113
Netzwerkdatenbanken, 264, 267, 269
nsswitch.conf-Datei, 267, 269
Standard-TCP/IP-Services, 142
Voraussetzungen, 102
VPN durch IPsec geschützt, 560-570
VPN im Transportmodus mit IPsec, 576-583
VPN im Tunnelmodus mit IPsec, 554, 560-570
Konfiguration von IKE (Übersicht der Schritte), 611
Konfiguration von IKE für mobile Systeme (Übersicht der Schritte), 642
Konfiguration von IKE mit PresharedKeys (Übersicht der Schritte), 612
Konfiguration von IKE mit PublicKey-Zertifikaten (Übersicht der Schritte), 624
Konfiguration von IKE zum Suchen angehängter Hardware (Übersicht der Schritte), 650
Konfigurationsdatei
IPv6
/etc/inet/ndpd.conf-Datei, 284-288
Konfigurationsdateien
für Oracle Solaris IP Filter erstellen, 715-716
IPv6
/etc/inet/hostname6.*Schnittstelle*-Datei, 288-289
/etc/inet/ipaddrsel.conf-Datei, 289
/etc/inet/ndpd.conf-Datei, 285, 286
Oracle Solaris IP Filter-Beispiele, 670
TCP/IP-Netzwerke
/etc/defaultdomain-Datei, 255
/etc/defaultrouter-Datei, 255
/etc/hostname.*Schnittstelle*-Datei, 254
/etc/nodename-Datei, 114, 255
hosts-Datenbank, 255, 258
netmasks-Datenbank, 260
Konfigurieren, IPsec, 594-595
Konnektivität, ICMP-Protokoll, Fehlerberichte, 41
kstat-Befehl, mit IPQoS verwenden, 904

L

-L-Option, ipsecconf-Befehl, 543
-l-Option
ikecert certdb-Befehl, 627
ipsecconf-Befehl, 543
Lastausgleich
in einem IPQoS-konformen Netzwerk, 844
in einem IPv6-konformen Netzwerk, 303
Lastausgleich für eingehende Daten, 303
Lastenausgleich, zwischen Aggregationen, 176
Lastverteilung
abgehend, 783
Definition, 780
Laufwerkslose Clients, Unterstützung von DHCP, 440
ldap-list-Schlüsselwort, IKE-Konfigurationsdatei, 642
Leasing-Zeit verlängern, 464
Leeren, *Siehe* löschen

Legacy-Schnittstellen, 166-167
Lesen, IPsec-Richtlinie, 542-543
Link, IPv6, 78
Link Aggregation Control Protocol (LACP)
  LACP-Modi modifizieren, 180
  Modi, 176
Link-lokale Adresse
  als eine IPMP-Testadresse, 785-786
  Format, 83
  mit einem Token manuell konfigurieren, 202
Link-lokale Adressen
  IPv6, 302, 305, 309
Link-lokale IPv6-Adresse, mit IPMP, 786
Linkaggregationen, *Siehe* Aggregationen
Liste
  Algorithmen (IPsec), 522, 600
  CRL (IPsec), 641
  Hardware (IPsec), 653
  Token-IDs (IPsec), 653
  Token-IDs von Metaslot, 653-654
  Zertifikate (IPsec), 627, 640
logische Domänen, IPsec und, 530
Logische Schnittstelle, 456
  Definition, 148, 165
Logische Schnittstellen, 457
  DHCP-Clientsysteme, 466
  für IPv6-Adresse, 288-289
  für IPv6-Tunnel, 205, 206, 207
Lokale Dateien als Namen-Service
  Beschreibung, 67
  lokale Dateien-Modus, 104, 105
  Netzwerkdatenbanken, 265
Lokale Dateien-Modus
  Definition, 103
  für Systeme erforderlich, 104
lokale Dateien-Modus
  für Systeme erforderlich, 105
  Host konfigurieren, 112
Lokale Dateien-Modus
  Netzwerkkonfigurationsserver, 104
Loopback-Adresse, 114, 257
Löschen
  DHCP-Optionen, 438
  IPsec SAs, 546

M

`-m`-Option, `ikecert certlocal`-Befehl, 625
MAC-Adresse, 455
  Einmaligkeit sicherstellen, 163-164
  in DHCP-Client-ID verwenden, 335
  in `ethers`-Datenbank einer IP-Adresse zuordnen, 270
  IPMP-Anforderungen, 783-784
  IPv6-Schnittstellen-ID, 82
Makros
  DHCP
    Siehe DHCP-Makros
`manual-key`-Service
  Beschreibung, 520, 593
  Verwenden, 538
Markermodule, 833
  Siehe auch `dlcosmk`-Marker
  Siehe auch `dscpmk`-Marker
  DS Codepoint angeben, 915
  PHBs, zur IP-Paketweiterleitung, 836
  Unterstützung für VLAN-Geräte, 915
`MaxClockSkew`-Label, 746, 767
Maximum Transmission Unit (MTU), 304
MD5-Authentifizierungsalgorithmus, Schlüssellänge, 547
Media Access Control (MAC)-Adresse, *Siehe* MAC-Adresse
Mehrere Netzwerkschnittstellen
  DHCP-Clientsysteme, 466
  `/etc/inet/hosts`-Datei, 257
  Routerkonfiguration, 126, 129
Metaslot
  Schlüsselspeicher, 603, 653-654
  Schlüsselspeicherung, 512
Metermodule
  Siehe auch `tokenmt`-Meter
  Siehe auch `tswtclmt`-Meter
  Einführung, 833
  Ergebnis der Messung, 833, 910
  in der IPQoS-Konfigurationsdatei aufrufen, 887
`mipagent.conf`-Konfigurationsdatei, 745, 746, 760, 773
  konfigurieren, 744
`mipagent`-Daemon, 745, 760, 775

mipagent_state-Datei, 775
mipagentconfig
-Befehl
Address-Abschnitt ändern, 753
Advertisements-Abschnitt ändern, 750
General-Abschnitt ändern, 749
GlobalSecurityParameters-Abschnitt ändern, 751
Pool-Abschnitt ändern, 751
SPI-Abschnitt ändern, 752
mipagentconfig-Befehl
ändern
Konfigurationsdatei, 749
Beschreibung der Befehle, 773
Mobility-Agent konfigurieren, 773
mipagentstat-Befehl
Agent-Status anzeigen, 756-757
Status des Mobility-Agent, 774
MN-FAauth-Label, 746, 767
Mobile-Foreign-Agent-Authentifizierung, 736
Mobile-Home-Agent-Authentifizierung, 736
Mobile IP
Abschnitt in Konfigurationsdatei, 764
Address-Abschnitt
Network Access Identifier, 771-772
standardmäßiger mobiler Knoten, 748, 772-773
Agent Advertisement-Nachrichten, 728, 729, 733
Agent-Erkennung, 729-730
Agent Solicitation, 728, 729, 730
Agent-Status anzeigen, 756-757
Antwort auf Registrierungsanforderung, 737
Arbeitsweise, 726-729
Bereitstellung, 743
Broadcast-Datagramme, 739
Datagrammbewegung, 725
drahtlose Kommunikation, 726, 730, 741
gekapseltes Datagramm, 726
Kapselungsarten, 738
Konfigurationsdatei
Address-Abschnitt, 768, 770-773
Advertisements-Abschnitt, 765-767
General-Abschnitt, 765
GlobalSecurityParameters-Abschnitt, 767-768
Pool-Abschnitt, 768-769
Mobile IP, Konfigurationsdatei *(Fortsetzung)*
SPI-Abschnitt, 769-770, 770, 771
Konfigurationsdateibeispiele, 761-764
Konfigurationsdateiformat, 761
konfigurieren, 744-748
Nachrichtenauthentifizierung, 736, 741, 769
Network Access Identifier, 770
nicht unterstützte Funktionen, 760
nicht unterstützte RFCs, 760
private Adressen, 732-733
Registrierung, 726, 728, 733
Registrierung aufheben, 729, 734, 735
Rücktunnel-Flag, 735
Registrierungsanforderung, 736
Registrierungsnachrichten, 734, 735, 736, 760
Router Advertisement-Nachrichten, 760
Routing von Multicast-Datagrammen, 740
Routing von Unicast Datagrammen, 739
Rücktunnel, 729, 731-733
Routing von Multicast-Datagrammen, 740
Überlegungen zum Foreign-Agent, 737
Überlegungen zum Home-Agent, 737
Unicast Datagramm-Routing, 739
Sicherheitsbetrachtungen, 741
Sicherheitszuordnungen, 736
Sicherheitszuordnungen (SPI), 736, 769
Statusinformationen, 775
unterstützte RFCs, 759
Mobile IP-Topologie, 724
Mobiler Knoten, 724, 725, 726, 771
Address-Abschnitt, 748
Definition, 726
Mobility-Agent, 728, 737
Address-Abschnitt, 770, 771
mipagent_state-Datei, 775
Router Advertisement-Nachrichten, 760
Software, 759, 773
Status, 774
Mobility-Bindung, 734, 736, 737, 739
mpathd-Datei, 820-822
Multicast-Adressen, IPv6
Format, 280-281
im Vergleich mit Broadcast-Adressen, 305
Übersicht, 83-84

Multihomed-Hosts
  aktivieren für IPv6, 186-188
  Beispielkonfiguration, 136
  Definition, 125, 134
  in Netzwerken mit Firewall, 135
  konfigurieren, 135-138
  während der Installation konfigurieren, 257

N

Nachrichten, Router Advertisement, 307
Nachrichtenauthentifizierung
  Mobile IP, 736, 769, 771
Nächster Hop, 305
Namen/Benennung
  Domain-Namen
    Registrierung, 38
  Domänennamen
    auswählen, 68
    Top-Level-Domain, 68
  Hostname
    `/etc/inet/hosts`-Datei, 257
    Verwaltung, 66
  Knotennamen
    lokaler Host, 114, 255
  Netzwerkentitäten benennen, 66, 69
Namen-Service lokale Dateien
  `/etc/inet/hosts`-Datei, 536
    Anforderungen, 258
    Beispiel, 258
    Format, 256
    ursprüngliche Datei, 256, 257
  `/etc/inet/ipnodes`-Datei, 536
Namen-Services
  Administrative Unterbereiche, 68
  Datenbank-Suchreihenfolge angeben, 267, 269
  den Netzwerkdatenbanken entsprechende
    Dateien, 266
  DHCP-Clients registrieren, 385
  Domain-Namen-Registrierung, 38
  Domain-Namen-System (DNS), 44, 67
  `hosts`-Datenbank und, 258
  lokale Dateien
    Beschreibung, 67
Namen-Services, lokale Dateien *(Fortsetzung)*
    `/etc/inet/hosts`-Datei, 256, 258
    lokale Dateien-Modus, 104, 105
  Netzwerkdatenbanken und, 67, 265
  NIS, 67
  NIS+, 67
  `nsswitch.conf`-Dateivorlagen, 268
  Service auswählen, 67, 69
  unterstützte Services, 67
NAT
  deaktivieren, 687
  Einschränkungen bei IPsec, 528-529
  IPsec unterstützt mehrere Clients, 511-513
  Konfigurationsregeln für, 674-675
  konform mit RFCs, 512
  mit IPsec und IKE, 647-648, 649
  NAT-Regeln
    anhängen, 704
    anzeigen, 703
  NAT-Regeln entfernen, 703-704
  Statistiken anzeigen, 709
  Übersicht, 674-675
`ndd`-Befehl, `pfil`-Modul anzeigen und, 694
`ndpd.conf`-Datei
  6to4-Advertisement-Nachrichten, 210
  erstellen, auf einem IPv6-Router, 194
`ndpd.conf`-Datei
  Schlüsselwortliste, 284-288
`ndpd.conf`-Datei
  temporäre Adressen konfigurieren, 198
`ndpd.conf`-Datei
  Variablen zur Präfixkonfiguration, 286
  Variablen zur Schnittstellenkonfiguration, 285
Neighbor Discovery-Protokoll
  Adressauflösung, 85
  Algorithmus zur Erkennung doppelt vorhandener
    Adressen, 303
  automatische Adresskonfiguration, 85, 300
  Hauptfunktionen, 299-306
  Leistungsmerkmale, 84
  Neighbor Solicitation, 302
  Präfix-Erkennung, 85, 301
  Router-Erkennung, 85, 301
  Vergleich mitARP, 304-306

Neighbor Solicitation, IPv6, 300
Neighbor-Unerreichbarkeitserkennung, IPv6, 85
Neighbor Unreachability Detection
  IPv6, 302, 305
`/net/if_types.h`-Datei, 801
`netmasks`-Datenbank, 260
  Datenbank Netzwerkmasken
    an IPv4-Adressen anwenden, 262
  entsprechende Namen-Service-Dateien, 266
  `/etc/inet/netmasks`-Datei
    bearbeiten, 262, 263
    Routerkonfiguration, 129
    Teilnetze hinzufügen, 106
  Netzwerkmasken
    an IPv4-Adressen anwenden, 262
    Beschreibung, 261
    erstellen, 261, 262
  Subnetting, 260
  Teilnetze hinzufügen, 106, 111
`netstat`-Befehl
  `-a`-Option, 229
  Beschreibung, 225
  `-f`-Option, 229
  `inet`-Option, 229
  `inet6`-Option, 229
  IPv6-Erweiterungen, 294
  Mobile IP-Erweiterungen, 775
  `-r`-Option, 231-232
  Softwareprüfungen durchführen, 248
  Statistiken nach Protokoll anzeigen, 226
  Status bekannter Routen anzeigen, 231-232
  Syntax, 225
Network Access Identifier
  Mobile IP, 770
  Mobile IP `Address`-Abschnitt, 771-772
Network Address Translation (NAT), *Siehe* NAT
Network Management-Rechteprofil, 552
Network Security-Rechteprofil, 551-552
`networks`-Datenbank
  entsprechende Namen-Service-Dateien, 267
  Übersicht, 271
Netzwerk-IPsec-Verwaltung (Rechteprofil), 552
Netzwerkbeispiel für IPQoS, 865
Netzwerkclient
  Hostkonfiguration, 114
  Netzwerkkonfigurationsserver für, 112
Netzwerkclient-Modus
  Definition, 103
  Hostkonfiguration, 114
  Übersicht, 105
Netzwerkclients
  als Netzwerkclients konfigurierte Systeme, 105
  `ethers`-Datenbank, 270
  Netzwerkkonfigurationsserver für, 104
Netzwerkdatenbanken, 264, 267
  Auswirkungen der Namen-Services auf, 265, 267
  `bootparams`-Datenbank, 269
  DNS-Boot- und Datendateien und, 265
  entsprechende Namen-Service-Dateien, 266
  `ethers`-Datenbank
    Einträge überprüfen, 248
    Übersicht, 270
  `hosts`-Datenbank
    Auswirkungen der Namen-Services auf, 258
    Einträge überprüfen, 248
    Namen-Services, Formen von, 265
    Übersicht, 255, 258
  `netmasks`-Datenbank, 260, 266
  `networks`-Datenbank, 271
  `nsswitch.conf`-Datei und, 264, 267, 269
  `protocols`-Datenbank, 272
  `Services`-Datenbank, 272
Netzwerkentwurf
  Domänennamen auswählen, 68
  Hosts benennen, 66
  IP-Adressierungsschema, 58, 66
  Teilnetze einrichten, 260
  Übersicht, 57
Netzwerkklassen, 63
  Adressierungsschema, 62, 63
  Bereich der verfügbaren Zahlen, 63
  IANA-Zuweisung von Netzwerknummern, 63
  Klasse A, 274
  Klasse B, 275
  Klasse C, 275
  Netzwerknummern verwalten, 58

Netzwerkkonfiguration
  Aufgaben bei der IPv4-Netzwerkkonfiguration, 108
  Hop, Beschreibung, 119
  Host-Konfigurationsmodi, 103
  IPv4-Netzwerktopologie, 106
  IPv6 auf einem Host aktivieren, 196-204
  IPv6-konforme Multihomed-Hosts, 186-188
  IPv6-Router, 192
  Konfiguration
    Netzwerkclients, 113
    Services, 142
  Netzwerkkonfigurationsserver einrichten, 112
  Router, 126
  Sicherheit konfigurieren, 509
  TCP/IP-Konfigurationsmodi, 106
    Konfigurationsinformationen, 103
    lokale Dateien-Modus, 105
    Netzwerkclient-Modus, 105
    Netzwerkkonfigurationsserver, 104
Netzwerkkonfigurationsserver
  Boot-Protokolle, 104
  Definition, 104
  einrichten, 112
Netzwerknummern, 38
Netzwerknummern der Klasse A, Bereich der verfügbaren Zahlen, 63
Netzwerknummern der Klasse A, B und C, 58, 63
Netzwerknummern der Klasse B, Bereich der verfügbaren Zahlen, 63
Netzwerknummern der Klasse C, Bereich der verfügbaren Zahlen, 63
Netzwerkplanung, 55, 72
  Designentscheidungen, 57
  IP-Adressierungsschema, 58, 66
  Namenszuweisungen, 66, 69
  Registrierung Ihres Netzwerks, 60
  Router hinzufügen, 69, 72
Netzwerkpräfix, IPv4, 64
Netzwerkschnittstelle, konfigurieren, 147-154
Netzwerkschnittstellen
  DHCP-Status anzeigen, 465
  durch DHCP-Service überwachen, 389
  IP-Adressen und, 65
Netzwerkschnittstellen *(Fortsetzung)*
  mehrere Netzwerkschnittstellen
    `/etc/inet/hosts`-Datei, 257
Netzwerkschnittstellenkarte (NIC)
  Ausfall und Failover, 782
  beim Systemstart fehlende NICs verwalten, 795-796
  Definition, 781
  dynamische Rekonfiguration, 783
  IPMP unterstützende NICs, 789
  NIC-Geschwindigkeit in einer IPMP-Gruppe, 782
  NICs, Arten, 148, 165
  NICs mit DR anschließen, 794
  NICs mit DR trennen, 794-795
  NICs mit DR wieder anschließen, 795
  Reparaturerkennung, 782-783
Netzwerkschnittstellennamen, 165-166
Netzwerksicherheit, konfigurieren, 509
Netzwerktopologie, 69, 70
  autonomes System, 123
  DHCP und, 338
Netzwerktopologiem für IPQoS, Konfigurationsbeispiel, 859
Netzwerktopologien für IPQoS, 842
  LAN mit IPQoS-konformen Hosts, 843
  LAN mit IPQoS-konformen Serverfarmen, 843
  LAN mit IPQoS-konformer Firewall, 844
Netzwerkverwaltung
  Hostnamen, 66
  Netzwerknummern, 58
  Simple Network Management Protocol (SNMP), 45
Netzwerkverwaltungadministration, Netzwerkentwurf, 57
Neue Funktionen
  DHCP auf logischen Schnittstellen, 466
  DHCP-Ereignisskripten, 473-476
  IKE-Erweiterungen, 610
  `inetconv`-Befehl, 113
  IPsec-Verbesserungen, 532
  Link-lokale Adresse manuell
    konfigurieren, 200-202
  Schnittstellenstatus mit dem `dladm`-Befehl, 158
  SCTP-Protokoll, 143-147
  Service Management Facility (SMF), 113
  Standard-Adressauswahl, 242-245

Neue Funktionen *(Fortsetzung)*
Standortpräfix, in IPv6, 79, 80-81
Stichproben-basierte Ausfallerkennung, 789
temporäre Adressen, in IPv6, 196-199
Zielsysteme in IPMP konfigurieren, 806-808
Neue Leistungsmerkmale, `routeadm`-Befehl, 193
next-hop, 119
NFS-Services, 45
NIC
Siehe Netzwerkschnittstellenkarte (NIC)
für Oracle Solaris IP Filter angeben, 691-692
Nicht verwendbare DHCP-Adresse, 406, 413
Nicht-VLAN-Schnittstellen, 166-167
NIS
als Namen-Service auswählen, 67
Domain-Namen-Registrierung, 38
IPv6-Adressen hinzufügen, 214-215
Netzwerkdatenbanken, 67, 265
NIS+
als Namen-Service auswählen, 67
und DHCP-Datenspeicher, 477-481
`nisaddcred`-Befehl, und DHCP, 480
`nischmod`-Befehl, und DHCP, 480
`nisls`-Befehl, und DHCP, 479
`nisstat`-Befehl und DHCP, 478
`nodename`-Datei
Beschreibung, 255
für den Netzwerkclient-Modus löschen, 114
`nslookup`-Befehl, 318
IPv6, 216
`nsswitch.conf`-Datei, 267, 269
ändern, 268, 269
Änderungen, zur IPv6-Unterstützung, 316-317
Beispiele, 268
Namen-Service-Vorlagen, 268
Netzwerkclient-Modus konfigurieren, 114
Syntax, 268

O

`od`-Befehl, 615
Öffentliche Topologie, IPv6, 82
Open Systems Interconnect (OSI)-Referenzmodell, 38, 39
OpenSolaris IP Filter
`ifconfig`-Befehl, 670
Richtlinien zur Verwendung, 670
`/opt/SUNWconn/lib/libpkcs11.so`-Eintrag, in `ike/config`-Datei, 660
Optionsanforderungen, 457
Oracle Solaris IP Filter
Adresspools
anhängen, 706
anzeigen, 705
entfernen, 705-706
Adresspools und, 675-677
Aktivieren in früheren Oracle Solaris 10-Versionen, 688-691
anzeigen
Adresspool-Statistiken, 709-710
NAT-Statistiken, 709
`pfil`-Statistiken anzeigen, 694
Protokolldateien, 711-713
Statusstatistiken, 708-709
Statustabellen, 707-708
Beispiel für Konfigurationsdatei, 670
deaktivieren, 687
Deaktivieren
auf einem NIC, 692-694
deaktivieren
NAT, 687
entfernen
NAT-Regeln, 703-704
erstellen
Protokolldateien, 710-711
`/etc/ipf/ipf.conf`-Datei, 715-716
`/etc/ipf/ipf6.conf`-Datei, 678-679
`/etc/ipf/ipnat.conf`-Datei, 715-716
`/etc/ipf/ippool.conf`-Datei, 715-716
`ipf`-Befehl, 683-684
`-6`-Option, 678-679
`ipf.conf`-Datei, 671-674
`ipf6.conf`-Datei, 678-679
`ipfstat`-Befehl
`-6`-Option, 678-679
`ipmon`-Befehl
IPv6 und, 678-679
`ipnat`-Befehl, 683-684

Oracle Solaris IP Filter *(Fortsetzung)*
- `ipnat.conf`-Datei, 674-675
- `ippool`-Befehl, 705
  - IPv6 und, 678-679
- `ippool.conf`-Datei, 675-677
- IPv6, 678-679
- Konfigurationsdateien erstellen, 715-716
- Loopback-Filterung, 684-685
- NAT-Regeln
  - anhängen, 704
  - anzeigen, 703
- neu aktivieren, 683-684
- NIC angeben, 691-692
- Open Source-Informationen, 667
- Paketfilter-Hooks, 677, 682-683
- Paketfilter-Regellisten verwalten, 696-702
- Paketfilterung, Übersicht, 671-674
- `pfil`-Modul, 677-678
- Protokolldatei leeren, 713
- protokollierte Pakete in einer Datei speichern, 713-714
- Regelliste
  - aktive, 696-697
  - andere Liste aktivieren, 697-699
  - einer aktive Liste Regeln hinzufügen, 699-700
  - einer inaktiven Liste Regeln hinzufügen, 700-701
  - entfernen, 699
  - inaktive, 697
  - inaktive Liste entfernen, 702
  - zwischen Listen wechseln, 701-702
- Regellisten und, 671-677
- Übersicht, 666-667

Oracle Solaris IP Filter deaktivieren, 687

P

Paket-Header, Funktionen des TCP-Protokolls, 42

Pakete
- abgeworfen oder verloren, 41, 233
- Beschreibung, 45
- Datenfluss prüfen, 238
- Datenkapselung, 46, 47
- Fragmentierung, 41
- Funktionen des IP-Protokolls, 40
- Header
  - Funktionen des TCP-Protokolls, 42
  - IP-Header, 48
- Inhalte anzeigen, 239
- IPv6-Header-Format, 281-282
- Lebenszyklus, 46, 49
  - Anwendungsschicht, 46
  - Bitübertragungsschicht, 48
  - Internetschicht, 48
  - Prozess auf dem empfangenden Host, 48, 49
  - Sicherungsschicht, 48
  - Transportschicht, 46, 47
- Schutz
  - abgehende Pakete, 516
  - eingehende Pakete, 516
  - mit IKE, 605
  - mit IPsec, 516, 520-524
- Schutz überprüfen, 550-551
- Übertragung
  - Router, 71, 72
  - TCP/IP-Stapel, 45, 49
- UDP, 47
- weiterleiten, 119

Paketfilter-Hooks, 677

Paketfilterung
- andere Regelliste aktivieren, 697-699
- deaktivieren, 686
- entfernen
  - aktive Regelliste, 699
  - inaktive Regelliste, 702
- hinzufügen
  - Regeln zu aktiver Liste, 699-700
  - Regeln zu inaktiver Liste, 700-701
- konfigurieren, 671-674
- nach dem Hochladen einer aktuellen Regelliste neu laden, 697-699
- NIC angeben, 691-692
- Regellisten verwalten, 696-702
- zwischen Regellisten wechseln, 701-702

Paketfluss
- durch Tunnel, 314
- Relay-Router, 315

Paketfluss, IPv6
 6to4 und native IPv6, 315
 durch 6to4-Tunnel, 314
params-Klausel
 für eine flowacct-Aktion, 876
 für eine Marker action, 873
 für eine Metermodul-action, 887
 globale Statistiken definieren, 869, 924
 Syntax, 924
Per-Hop-Behavior (PHB), 836
 AF-Weiterleitung, 837
 EF-Weiterleitung, 837
 in der IPQoS-Konfigurationsdatei definieren, 889
 mit dscpmk-Marker verwenden, 913
Perfect Forward Secrecy (PFS)
 Beschreibung, 605
 IKE, 604
PF_KEY Socket-Schnittstelle, IPsec, 519
PF_KEY-Socket-Schnittstelle, IPsec, 531
pfil-Modul, 677-678
 Statistiken anzeigen, 694
PFS, *Siehe* Perfect Forward Secrecy (PFS)
Physikalische Schnittstelle, 173-174
 Siehe auch Schnittstellen
 Ausfallerkennung, 789
 Benennungskonventionen, 165-166
 Definition, 148, 165, 781
 entfernen, 162
  in Solaris 10 3/05, 151-152
 konfigurieren, 147-154
 nach der Installation hinzufügen, 149, 159
 Netzwerkschnittstellenkarte (NIC), 148, 165
 Reparaturerkennung mit IPMP, 791
 VLANs, Definition, 152-154
Physikalischer Anschlusspunkt (Physical Point Of Attachment, PPA), 154, 169
ping-Befehl, 233
 Ausführen, 233
 Beschreibung, 232
 Erweiterungen für IPv6, 295
 -s-Option, 233
 Syntax, 232
PKCS #11-Bibliothek
 in ike/config-Datei, 660
PKCS #11-Bibliothek *(Fortsetzung)*
 Pfad zur Bibliothek angeben, 662
pkcs11_path-Schlüsselwort
 Beschreibung, 660
 ikecert-Befehl und, 662
 verwenden, 636
Platz sparender Modus, in.routed-Daemon, Option, 273
Platzhalter in bootparams-Datenbank, 270
Plumben einer Schnittstelle, 127, 149, 159
pntadm-Befehl
 Beispiele, 402
 Beschreibung, 331, 497
 in Skripten ausführen, 498
policy-Service
 Beschreibung, 593
 Verwenden, 537
Pool-Abschnitt
 Label und Werte, 768
 Mobile IP-Konfigurationsdatei, 768-769
Pool-Label, 748, 753, 772, 773
Ports, TCP-, UDP- und SCTP-Portnummern, 272
PPP-Links
 Fehlerbehebung
  Paketfluss, 238
Präfix
 Netzwerk, IPv4, 64
 Standortpräfix, IPv6, 80-81
 Teilnetzpräfix, IPv6, 81
Präfix-Erkennung, in IPv6, 85
Präfixe
 Router Advertisement-Nachricht, 301
 Router Advertisement-Nachrichten, 304, 307
PrefixFlags-Label, 746, 765
Preshared Schlüssel (IPsec), erstellen, 545-549
PresharedKeys (IKE)
 Anzeigen, 618-619
 Beschreibung, 606
 ersetzen, 616-617
 mit anderen Plattformen nutzen, 616
 speichern, 660
 Übersicht der Schritte, 612
Primäre Netzwerkschnittstelle, 148, 165
Private Adressen, Mobile IP, 732-733

Private Keys, speichern (IKE), 661
Privilegstufe
  Ändern in IKE, 618
  Festlegen in IKE, 623
  in IKE überprüfen, 617
  Prüfen in IKE, 618
protocols-Datenbank
  entsprechende Namen-Service-Dateien, 267
  Übersicht, 272
Protokolldatei, in Oracle Solaris IP Filter leeren, 713
Protokolldateien
  für Oracle Solaris IP Filter anzeigen, 711-713
  für Oracle Solaris IP Filter erstellen, 710-711
Protokollierte Pakete, in Datei speichern, 713-714
Protokollschichten
  OSI-Referenzmodell, 38, 39
  Paket-Lebenszyklus, 46, 49
  TCP/IP-Protokollarchitektur, Modell, 39, 45
    Anwendungsschicht, 39, 42, 45
    Bitübertragungsschicht, 39, 40
    Sicherungsschicht, 39, 40
    Transportsteuerungsschicht, 39, 41
    Vermittlungsschicht, 39, 40
Protokollstatistikanzeige, 226
proxy-Schlüsselwort, IKE-Konfigurationsdatei, 642
Prüfen
  IPsec-Konfigurationsdateien
    Syntax, 512
Public Key-Zertifikate, *Siehe* Zertifikate
PublicKeys, speichern (IKE), 663
publickeys Datenbank, 663

Q

-q-Option, in.routed-Daemon, 273
QoS-Richtlinie, 829
  Filter erstellen, 850
  in der IPQoS-Konfigurationsdatei umsetzen, 863
  Übersicht der Planung, 846
  Vorlage zur Richtlinienorganisation, 845
Quality Of Service (QoS)
  Aufgaben, 825
  QoS-Richtlinie, 828

R

„r"-Befehle, in UNIX, 44
RARP-Protokoll
  Beschreibung, 104
  Ethernet-Adressen überprüfen, 248
  Ethernet-Adresszuordnung, 270
  RARP-Server konfigurieren, 112
RBAC
  IPsec und, 535
  und DHCP-Befehle, 331
RDISC
  Beschreibung, 45, 274
Rechteprofile
  Network Management, 552
  Netzwerk-IPsec-Verwaltung, 552
Reconfiguration Coordination Manager
  (RCM)-Framework, 795
Redirect
  IPv6, 300, 305
Regelliste
  inaktive
    Siehe auch Oracle Solaris IP Filter
Regellisten
  Siehe siehe Oracle Solaris IP Filter
  NAT, 674-675
  Paketfilterung, 671-677
Registrieren
  autonome Systeme, 125
  Domain-Namen, 38
Registrierung
  Anforderung, 736
  Antwortnachricht, 737
  Mobile IP, 726, 728, 733
  Nachrichten, 734, 737
  Netzwerke, 60
  Rücktunnel-Flag, 735
Registrierung aufheben
  Mobile IP, 729, 734, 735
RegLifetime-Label, 746, 766
Regulierung der Bandbreite, 830
Relay-Router, 6to4-Tunnel konfigurieren, 211, 213
Reparaturerkennung, mit IPMP, 782-783, 791
Replay-Schutz, 767
ReplayMethod-Label, 747, 769

Requests for Comments (RFCs), 51
- Definition, 50
- IKE, 514
- IPQoS, 827
- IPsec, 514
- IPv6, 75-76

retry_limit-Schlüsselwort,
- IKE-Konfigurationsdatei, 655

retry_timer_init-Schlüsselwort,
- IKE-Konfigurationsdatei, 655

retry_timer_max-Schlüsselwort,
- IKE-Konfigurationsdatei, 655

Reverse Zone-Datei, 214
ReverseTunnel-Label, 746, 766
ReverseTunnelRequired-Label, 746, 766
Richtlinien, IPsec, 524
Richtlinien, für Aggregationen, 176
Richtliniendateien
- ike/config-Datei, 531, 609, 658
- ipsecinit.conf-Datei, 595-596
- Sicherheitsbetrachtungen, 596

rlogin Befehl, Paketprozess, 46
Rollen, Network Security-Rolle erstellen, 551-552
route-Befehl
- inet6-Option, 295
- IPsec, 564, 566, 574, 575, 580, 581, 586, 587

routeadm-Befehl
- dynamisches Routing aktivieren, 129, 141
- IPv6-Router Konfiguration, 193
- Multihomed-Hosts, 135

routeadm command, IP forwarding, 561
Router
- Adressen für DHCP-Clients, 346
- Beispiel, Konfiguration eines
  - Standard-Routers, 130
- Definition, 119, 126, 273
- dynamisches Routing, 141
- /etc/defaultrouter-Datei, 255
- Grenze, 124
- hinzufügen, 69, 72
- Konfiguration
  - für IPv4-Netzwerke, 126
  - Netzwerkschnittstellen, 129
- konfigurieren, 273

Router, konfigurieren *(Fortsetzung)*
  - IPv6, 192
- lokale Dateien-Modus konfigurieren, 111
- Netzwerktopologie, 69, 70
- Paketübertragung, 71, 72
- Probleme beim Aufrüsten auf IPv6, 249
- Rolle, in der 6to4-Topologie, 312
- Router zur Paketweiterleitung, 125
- Routing-Protokolle
  - automatische Auswahl, 129
  - Beschreibung, 45, 273, 274
- Standard-Router, 125
- Standardadresse, 109
- statisches Routing, 139

Router Advertisement-Nachricht, Präfix, 301
Router Advertisement-Nachrichten, 459
- IPv6, 299, 301, 304, 307
- Mobile IP, 760

Router-Erkennung, in IPv6, 85, 304
Router-Erkennung, unter IPv6, 296, 301
Router Solicitation
- IPv6, 299, 301

Router zur Paketweiterleitung, 125
Routing
- auf Multihomed-Hosts, 134
- Definition, 119
- direkte Route, 119
- dynamisches Routing, 131
- Gateway, 131
- indirekte Route, 119
- IPv6, 306
- Routing-Tabelle konfigurieren, 133
- Routing-Tabelle manuell konfigurieren, 131
- statisches Routing, 131
- statisches Routing konfigurieren, 138

Routing Information Protocol (RIP)
- Beschreibung, 45, 273

Routing-Protokolle
- automatische Auswahl, 129
- Beschreibung, 45, 119, 273, 274
- Border Gateway Protocol (BGP), 124
- Exterior Gateway Protocol (EGP), 120
- in Oracle Solaris, 120
- Interior Gateway Protocol (IGP), 120

Routing-Protokolle *(Fortsetzung)*
RDISC
Beschreibung, 45, 274
RIP
Beschreibung, 45, 273
zugehörige Routing-Daemons, 120-121
Routing-Tabellen
alle Routen verfolgen, 238
anzeigen, 247
Beispiel für die Paketübertragung, 72
Beschreibung, 71
Definition, 119
`in.routed`-Daemon, Erstellung, 273
manuell konfigurieren, 131, 133
Platz sparender Modus, 273
Subnetting und, 260
Routing von Multicast-Datagrammen, Mobile IP, 740
Routing von Unicast Datagrammen, Mobile IP, 739
`rpc.bootparamd`-Daemon, 105
RSA-Verschlüsselungsalgorithmus, 662
Rücktunnel
Mobile IP, 729, 731-733
Routing von Multicast-Datagrammen, 740
Überlegungen zum Foreign-Agent, 737
Überlegungen zum Home-Agent, 737
Unicast Datagramm-Routing, 739

S

`-S`-Option
`ikecert certlocal`-Befehl, 626
`in.routed`-Daemon, 273
`-s`-Option, `ping`-Befehl, 233
Schlüssel
auf Hardware speichern, 608
automatische Verwaltung, 604
für IPsec SAs erstellen, 545-549
`ike.privatekeys`-Datenbank, 663
`ike/publickeys` Datenbank, 663
in IPsec verwalten, 519-520
manuelle Verwaltung, 598-599
Preshared (IKE), 606
speichern (IKE)
privat, 661
Schlüssel, speichern (IKE) *(Fortsetzung)*
PublicKeys, 663
Zertifikate, 663
Zufallszahlen erzeugen für, 543-544
Schlüssel-Dienstprogramm, IKE-Programm, 604
Schlüssel-Dienstprogramme
`ike`-Service, 520
`ipseckey`-Befehl, 520
`manual-key`-Service, 520
Schlüsselaushandlung, IKE, 654-656
Schlüsselmanagement
automatisch, 604
IKE, 604
`ike`-Service, 520
IPsec, 519-520
`manual-key`-Service, 520
manuell, 598-599
Zonen und, 535
Schlüsselspeicher
IPsec SAs, 531
ISAKMP SAs, 660
Softtoken, 660
Softtoken-Schlüsselspeicher, 653-654
Token-IDs von Metaslot, 653-654
Schlüsselspeicher-Name, *Siehe* Token-ID
Schlüsselspeicherung,
Softtoken-Schlüsselspeicher, 512
Schnittstelle, Definition, 165
Schnittstelle plumben (aktivieren), 166
Schnittstellen
Arten von NICs, 148, 165
Benennungskonventionen, 165-166
Einmaligkeit der MAC-Adresse prüfen, 163-164
entfernen, 151-152
unter Solaris 10 1/06, 162
Failover, mit IPMP, 791
IPMP-Schnittstellentypen, 787-788
Konfiguration
als Teil eines VLAN, 171-173
logische IPv6-Schnittstellen, 288-289
manuell, für IPv6, 186-188
plumben, 166
temporäre Adresse, 196-199
unter Solaris 10 1/06, 159-162

Schnittstellen, Konfiguration *(Fortsetzung)*
unter Solaris 10 3/05, 149
zu Aggregationen, 177-179
Legacy-Schnittstellentypen, 166-167
manuell konfigurieren, für IPv6, 186-188
Multihomed-Hosts, 134, 257
nicht-VLAN-Schnittstellentypen, 166-167
Pakete prüfen, 239-240
Pseudoschnittstelle, für 6to4-Tunnel, 208
Reihenfolge der STREAMS-Module an einer Schnittstelle, 800
Routerkonfiguration, 126, 129
Standby, in IPMP, 787-788, 808-810
Status anzeigen, 221, 224, 788
Status anzeigen, unter Solaris 10 1/06, 157-158
Typen, die Aggregationen unterstützen, 177
Typen, unter Solaris 10 1/06, 166-167
VLANs, 167-173
VLANs, unter Solaris 10 3/05, 152-154
Schnittstellen-ID
Definition, 82
Format, in einer IPv6-Adresse, 79
manuell konfiguriertes Token verwenden, 202
Schützen
IPsec-Verkehr, 513
mobile Systeme mit IPsec, 643-650
Pakete zwischen zwei Systemen, 535-539
Schlüssel in Hardware, 608
VPN mit IPsec-Tunnel im Transportmodus, 576-583
VPN mit IPsec-Tunnel im Tunnelmodus, 560-570
Webserver mit IPsec, 539-542
Schützen des Datenverkehrs mit IPsec (Übersicht der Schritte), 533
Schutzmechanismen, IPsec, 520-524
SCTP-Protokoll
Beschreibung, 42
Einschränkungen mit IPsec, 529
IPsec und, 535
SCTP-konforme Services hinzufügen, 143-147
Services in `/etc/inet/services`-Datei, 272
Statistiken anzeigen, 226
Status anzeigen, 227-228
Security Parameter Index (SPI)
Beschreibung, 519-520
konstruieren, 544
Mobile IP, 736, 769
Schlüsselgröße, 544
Security Policy Database (SPD), konfigurieren, 594
Security Policy-Datenbank (SPD)
IPsec, 513, 515
Selektoren, 832
IPQoS 5-Tuple, 832
Liste der Selektoren, 908
Planung, in der QoS-Richtlinie, 850
Sendender Host
Paketpfad durch, 46, 48
Server, DHCPv6, 454
Server, IPv6
Aufgaben planen, 94-95
IPv6 aktivieren, 202-204
Service-Level Agreement (SLA), 828
Rechnungen für Kunden erstellen, basierend auf dem Flow Accounting, 902
Serviceklassen, 832
unterschiedliche Serviceklassen bereitstellen, 830
Service Management Facility (SMF)
IKE-Service
Aktivieren, 537, 646, 656, 658
Aktualisieren, 538, 617
Ändern`admin_privilege` Service-Eigenschaft, 618
Beschreibung, 603, 657-658
`ike`-Service, 520, 608
Konfigurierbare Eigenschaften, 657
Neu starten, 537
IPsec-Service
`manual-key`-Service, 598
IPsec-Services, 593-594
Beschreibung, 511-513
`ipsecalgs`-Service, 597
Liste, 530-532
`manual-key`-Beschreibung, 520
`manual-key`-Verwendung, 538
`policy`-Service, 530
Verwalten von IKE, 553-554
Verwalten von IPsec, 553-554

Serviceklasse (Class of Service, CoS)-Marker, 833
Serviceklassen, *Siehe* Klassen
Services
  Netzwerk und der Befehl `svcadm`, 561, 572, 577
`Services`-Datenbank
  aktualisieren, für SCTP, 144
  entsprechende Namen-Service-Dateien, 267
  Übersicht, 272
Sicherheit
  IKE, 658
  IPsec, 513
Sicherheits-Richtlinie, `ipsecinit.conf`-Datei (IPsec), 536
Sicherheitsbetrachtungen
  Authentication Header (AH), 522
  Encapsulating Security Payload (ESP), 522
  gesperrte Sockets, 596
  `ike/config`-Datei, 658
  `ipsecconf`-Befehl, 596
  `ipsecinit.conf`-Datei, 596
  `ipseckey`-Befehl, 598-599
  `ipseckeys`-Datei, 548
  IPv6-konforme Netzwerke, 97-98
  Konfiguration
    IPsec, 536
  Mobile IP, 741
  Preshared-Schlüssel, 607
  Probleme mit 6to4-Relay-Router, 250
  Sicherheitsprotokolle, 522
Sicherheitsprotokolle
  Authentication Header (AH), 520-521
  Encapsulating Security Payload (ESP), 521-522
  IPsec-Schutzmechanismen, 520
  Sicherheitsbetrachtungen, 522
  Übersicht, 513
Sicherheitsrichtlinie
  `ike/config`-Datei (IKE), 531
  IPsec, 524
  `ipsecinit.conf`-Datei (IPsec), 595-596
Sicherheitszuordnung-Datenbank (SADB), 597
Sicherheitszuordnungen, Mobile IP, 736
Sicherheitszuordnungen (SAs)
  IKE, 658
  IPsec, 519-520, 537
Sicherheitszuordnungen (SAs) *(Fortsetzung)*
  IPsec-Datenbank, 597
  IPsec hinzufügen, 537
  IPsec SAs ersetzen, 546
  IPsec SAs leeren, 546
  ISAKMP, 605
  manuell erstellen, 545-549
  Schlüssel erzeugen für, 543-544
  Zufallszahlerzeugung, 606
Sicherungsschicht
  Framing, 48
  OSI, 39
  Paket-Lebenszyklus
    empfangender Host, 48
    sendender Host, 48
  TCP/IP, 39, 40
Sicherungsschichtadresse ändern, 304
Simple Network Management Protocol (SNMP), 45
Sitzungsschicht
  Paket-Lebenszyklus
    empfangender Host, 49
Sitzungsschicht (OSI), 39
`Size`-Label, 747, 769
Slots, in Hardware, 663
SNMP (Simple Network Management Protocol), 45
`snoop`-Befehl
  DHCP-Verkehr überwachen, 485-486
    Beispielausgabe, 490
  Erweiterungen für IPv6, 294
  geschützte Pakete anzeigen, 599, 601
  `ip6`-Protokollschlüsselwort, 294
  IPv6-Verkehr überwachen, 241-242
  Mobile IP-Erweiterungen, 776
  Pakete zwischen Server und Client prüfen, 241
  Paketfluss prüfen, 238
  Paketinhalte anzeigen, 239
  Paketschutz überprüfen, 550-551
Sockets
  IPsec-Sicherheit, 596
  Sicherheitsbetrachtungen, 539
  Socketstatus anzeigen mit `netstat`, 229
Softtoken-Schlüsselspeicher
  Schlüsselspeicher mit Metaslot, 603, 653-654, 660
  Schlüsselspeicherung mit Metaslot, 512

Solaris Cryptographic Framework, IPsec, und, 597
Solaris IP Filter, NAT und, 674-675
Speichern
  IKE-Schlüssel auf Datenträger, 632, 663
  IKE-Schlüssel auf Hardware, 608, 652-654
SPI-Abschnitt
  Label und Werte, 769
  Mobile IP-Konfigurationsdatei, 769-770, 770, 771
SPI-Label, 752, 770, 772, 773
Standard-Adressauswahl, 289-290
  Definition, 242-245
  Richtlinientabelle zur IPv6-Adressauswahl, 243-244
Standard-Router
  Beispielkonfiguration, 130
  Definition, 125
Standardmäßiger mobiler Knoten
  Mobile IPAddress-Abschnitt, 748, 772-773
standby-Parameter
  ifconfig-Befehl, 787, 809
Standby-Schnittstelle
  Definition, 787-788
  für eine IPMP-Gruppe konfigurieren, 808-810
  Testadresse auf Standby-Schnittstelle
    konfigurieren, 809
Standort-lokale Adressen, IPv6, 87
Standortpräfix, IPv6
  beziehen, 98
  Definition, 79, 80
  dem Router ankündigen, 194
Standorttopologie, IPv6, 82
Statisches Routing, 139, 255
  auf einem Host manuell konfigurieren, 138
  Beispiel einer Hostkonfiguration, 139
  Beispielkonfiguration, 134
  Eignung für, 132
  statische Route hinzufügen, 131, 133-134
Statistiken
  nach Protokoll (netstat), 226
  Paketübertragung (ping), 233
Statistiken für IPQoS
  globale Statistiken aktivieren, 923
  globale Statistiken ermöglichen, 869
  klassenbasierte Statistiken aktivieren, 923
  mit dem kstat-Befehl erzeugen, 904
Statusfreie automatische Adresskonfiguration, 301
Statusinformationen, Mobile IP, 775
Statusstatistiken, anzeigen, 708-709
Statustabellen, anzeigen, 707-708
Sternchen (*), -Platzhalter in
  bootparams-Datenbank, 270
Stichproben an Ziele senden, in.mpathd-Daemon, 784
Stichproben-basierte Ausfallerkennung
  Definition, 789, 790-791
  Stichprobenverkehr, IPMP, 784
  Stichprobenziele, 790
  Zielsysteme konfigurieren, 806-808
Stichprobenbasierte Fehlererkennung, Failure
  Detection Time, 790
Sun Crypto Accelerator 1000 Board, 608
Sun Crypto Accelerator 1000-Board, Mit IKE
  verwenden, 651-652
Sun Crypto Accelerator 4000-Board
  IKE-Schlüssel speichern, 608
  Mit IKE verwenden, 652-654
Sun Crypto Accelerator 4000Board, IKE-Berechnungen
  beschleunigen, 608
svcadm Befehl
  Aktualisieren von IKE, 622
svcadm-Befehl
  Netzwerkservices deaktivieren, 561, 572, 577
svcadm Befehl
  Neustart der IPsec-Richtlinie, 622
Switch-Konfiguration
  in einer Aggregation-Topologie, 174
  in einer VLAN-Topologie, 168
  LACP-Modi, 180
  Link Aggregation Control Protocol
    (LACP)-Modi, 176
Symbolische Namen für Netzwerknummern, 263
SYN-Segment, 47
sys-unconfig-Befehl
  und DHCP-Client, 462, 463
syslog.conf-Datei, Protokollierung für IPQoS, 896
Systeme, Kommunikation schützen, 535-539

T

-T-Option
  ikecert-Befehl, 637, 662, 663
  ikecert certlocal-Befehl, 626
-t-Option
  ikecert-Befehl, 662
  ikecert certlocal-Befehl, 625
  inetd-Daemon, 142
TCP/I-Netzwerke, IPv4-Netzwerktopologie, 106
TCP/IP-Netzwerke
  Aufgaben bei der IPv4-Netzwerkkonfiguration, 108
  Fehlerbehebung, 241
    ifconfig-Befehl, 221
    netstat-Befehl, 225
    Paketinhalte anzeigen, 239
    Paketverlust, 233
    ping-Befehl, 232, 233
  Fehlersuche
    allgemeine Methoden, 247, 248
    Diagnoseprogramme von Drittanbietern, 247
    Softwareprüfungen, 248
  Host-Konfigurationsmodi, 103, 106
    Beispielnetzwerk, 105
    gemischte Konfigurationen, 105
    lokale Dateien-Modus, 104, 105
    Netzwerkclient-Modus, 105
    Netzwerkkonfigurationsserver, 104
  Konfiguration
    Host-Konfigurationsmodi, 103, 106
    lokale Dateien-Modus, 112
    Netzwerkclients, 113
    Netzwerkdatenbanken, 264, 267, 269
    nsswitch.conf-Datei, 267, 269
    Standard-TCP/IP-Services, 142
    Voraussetzungen, 102
  Konfigurationsdateien, 253
    /etc/defaultdomain-Datei, 255
    /etc/defaultrouter-Datei, 255
    /etc/hostname.*Schnittstelle*-Datei, 254
    /etc/nodename-Datei, 114, 255
    hosts-Datenbank, 255, 258
    netmasks-Datenbank, 260
  konfigurieren
    Netzwerkkonfigurationsserver einrichten, 112
TCP/IP-Netzwerke *(Fortsetzung)*
  mit ESP schützen, 521
  Netzwerknummern, 38
TCP/IP-Protokoll-Suite, Dual-Stack-Protokolle, 93
TCP/IP-Protokollfamilie, 37
  Datenkommunikation, 45, 49
    Datenkapselung, 45, 49
  Internal Trace-Unterstützung, 49
  OSI-Referenzmodell, 38, 39
  Standardservices, 142
  Statistiken anzeigen, 226
  TCP/IP-Protokollarchitektur, Modell, 39, 45
    Anwendungsschicht, 39, 42, 45
    Bitübertragungsschicht, 39, 40
    Sicherungsschicht, 39, 40
    Transportschicht, 39, 41
    Vermittlungsschicht, 39, 40
  Übersicht, 37, 38
  Weitere Informationen, 49
    Bücher, 49
    FYIs, 50
TCP-Protokoll
  Beschreibung, 42
  Herstellen einer Verbindung, 47
  Segmentierung, 47
  Services in /etc/inet/services-Datei, 272
  Statistiken anzeigen, 226
TCP-Wrapper, aktivieren, 147
Teilnetze
  IPv4
    Netzmasken konfigurieren, 111
  IPv4-
    Adressen und, 261
  IPv4-Adressen und, 262
  IPv6
    6to4-Topologie und, 313
    Definition, 78
    Nummerierung vorschlagen, 98-99
  netmasks-Datenbank, 260
    bearbeiten/etc/inet/netmasks-Datei, 262, 263
    Netzwerkmaske erstellen, 261, 262
  Netzwerkkonfigurationsserver, 104
  Netzwerkmasken
    an IPv4-Adressen anwenden, 262

Teilnetze, Netzwerkmasken *(Fortsetzung)*
An IPv4-Adressen anwenden, 262
erstellen, 262
Teilnetznummer, IPv4, 260
Teilnetznummer in IPv4-Adressen, 63
Teilnetzpräfix, IPv6, 81
Übersicht, 260
Teilnetzpräfix, IPv6, 81
Telnet-Protokoll, 43
Temporäre Adresse, in IPv6
Definition, 196-199
konfigurieren, 197-199
`test`-Parameter, `ifconfig`-Befehl, 802
Testadressen, IPMP
Definition, 784
IPv4-Anforderungen, 785
IPv6- Anforderungen, 785-786
Konfiguration
auf einer Standby-Schnittstelle, 809
IPv4, 802
konfigurieren
IPv6, 803
Standby-Schnittstelle, 788
Stichprobenverkehr und, 784
Verwendung durch Anwendungen verhindern, 786
`tftp` Protokoll
Beschreibung, 43
Netzwerkkonfigurationsserver, Boot-Protokoll, 104
`/tftpboot`-Verzeichnis, erstellen, 112
Token-ID, in Hardware, 663
Token Ring, IPMP-Unterstützung für, 801
`tokenmt`-Meter, 833
Farberkennung konfigurieren, 833, 911
Messraten, 910
rate-Parameter, 911
Single-Rate Meter, 911
Two Rate-Meter, 911
`Tokens` Argument, `ikecert` Befehl, 661
Topologie, 69, 70
`traceroute`-Befehl
Definition, 237-238
Erweiterungen für IPv6, 295
Routen verfolgen, 238
Traffic-Konformität, Ergebnis, 833
Transportmodus
IPsec, 525-527
mit AH geschützte Daten, 526
mit ESP geschützte Daten, 526
Transportschicht
Datenkapselung, 46, 47
OSI, 39
Paket-Lebenszyklus
empfangender Host, 49
sendender Host, 46, 47
TCP/IP
Beschreibung, 39, 41
SCTP-Protokoll, 42, 143-147
TCP-Protokoll, 42
UDP-Protokoll, 42
Transportprotokollstatus beziehen, 227-228
Triple-DES-Verschlüsselungsalgorithmen, IPsec und, 523
Trunking, *Siehe* Aggregationen
`tswtclmt`-Meter, 833, 912
Messraten, 912
`tun`-Modul, 309
Tunnel
6to4-Tunnel, 312
bekannte Probleme, 251
Paketfluss, 314, 315
Topologie, 312
`ifconfig`Sicherheitsoptionen, 599-601
IPsec, 527
IPv6, automatische
Siehe Tunnel, 6to4-Tunnel
IPv6, manuell konfiguriert, 309-311
IPv6 konfigurieren
6to4-Tunnel, 208
Beispiele, 293
IPv4 über IPv6, 207
IPv6-über-IPv6, 206
zu einem 6to4-Relay-Router, 211
IPv6-Tunneling-Mechanismus, 308
Konfigurieren von IPv6
IPv6 über IPv4, 205-206
Modi in IPsec, 525-527
Pakete schützen, 527
Planung, für IPv6, 96-97

Tunnel *(Fortsetzung)*
- Topologie, zu einem 6to4-Relay-Router, 315
- Transportmodus, 525
- Tunnelmodus, 525

`Tunnel` Schlüsselwort, IPsec-Richtlinie, 525
`tunnel`-Schlüsselwort
- IPsec-Richtlinie, 555, 562, 572

Tunneling, 726, 738, 741
Tunnelmodus
- gesamtes inneres IP-Paket schützen, 526
- IPsec, 525-527

`Type`-Label, 753, 770, 772, 773

U

Übergang zu IPv6, 6to4-Mechanismus, 312
Überprüfen
- Datei `ipsecinit.conf`
  - Syntax, 563
- `ipsecinit.conf`-Datei
  - Syntax, 537
- Paketschutz, 550-551

Übersicht der Schritte
- DHCP
  - Ändern von DHCP-Service-Optionen, 375
  - BOOTP-Clients unterstützen, 399
  - DHCP-Server-Konfigurationsdaten verschieben, 446
  - Entscheidungen bei der IP-Adressverwaltung, 346
  - Entscheidungen bei der Konfiguration eines DHCP-Servers, 342
  - mit DHCP-Makros arbeiten, 419
  - mit DHCP-Netzwerken arbeiten, 388
  - mit DHCP-Optionen arbeiten, 430
  - mit IP-Adressen arbeiten, 402
  - Netzwerk für DHCP vorbereiten, 338
  - Unterstützung des Remote-Booting und laufwerkslosen Clients mit DHCP, 441
  - Unterstützung von Clients ausschließlich mit Informationen, 442
- IKE für mobile Systeme konfigurieren, 642
- IKE konfigurieren, 611
- IKE mit PresharedKeys konfigurieren, 612

Übersicht der Schritte *(Fortsetzung)*
- IKE mit PublicKey-Zertifikaten konfigurieren, 624
- IKE-Übertragungsparameter ändern, 654
- IKE zum Suchen angehängter Hardware konfigurieren, 650
- IPMP
  - dynamische Rekonfiguration (DR), Verwaltung, 799
  - IPMP-Gruppe, Konfiguration, 798-799
- IPQoS
  - Flow Accounting einrichten, 901
  - Konfigurationsdatei erstellen, 863
  - QoS-Richtlinie planen, 846
- IPv4-Netzwerk
  - Teilnetze hinzufügen, 106-107
- IPv6
  - konfigurieren, 191-192
  - Planung, 89-91
  - Tunnelkonfiguration, 204
- Mobile IP
  - Konfiguration ändern, 748-749
  - konfigurieren, 743-744
- Netzwerkkonfiguration, 102-103
- Netzwerkverwaltungsaufgaben, 220
- Schützen des Datenverkehrs mit IPsec (Übersicht der Schritte), 533
- VPN mit IPsec schützen (Übersicht der Schritte), 557-591

Übertragungsparameter
- globale IKE-Parameter, 655
- IKE einstellen, 654-656

Übertragungsparameter (IKE), ändern, 654
UDP-Protokoll
- Beschreibung, 42
- Services in `/etc/inet/services`-Datei, 272
- Statistiken anzeigen, 226
- UDP-Paketprozess, 47

UltraSPARC T2-Prozessor, Mit IKE verwenden, 651
Umgehen
- IPsec auf LAN, 562, 578
- IPsec-Richtlinie, 524

Umleitung, IPv6, 85
Uniform Resource Indicator (URI), für Zugriff auf CRLs, 640

UNIX „r“-Befehle, 44
Unterbereiche, administrative, 68
use_http-Schlüsselwort,
IKE-Konfigurationsdatei, 642
/usr/sbin/6to4relay-Befehl, 212
/usr/sbin/in.rdisc-Programm, Beschreibung, 274
/usr/sbin/in.routed-Daemon
Beschreibung, 273
Platz sparender Modus, 273
/usr/sbin/inetd-Daemon
Status von inetd prüfen, 248
vom Daemon gestartete Services, 142
/usr/sbin/ping-Befehl, 233
Ausführen, 233
Beschreibung, 232
Syntax, 232

V

-V-Option
snoop-Befehl, 599, 601
/var/inet/ndpd_state.Schnittstelle-Datei, 296
Verhindern von IP-Spoofing, SMF-Manifest, 589-591
Verkehr weiterleiten
Auswirkungen von PHBs auf die
Paketweiterleitung, 913
IP-Paketweiterleitung, mit DSCP, 836
Planung, in der QoS-Richtlinie, 849
Verkehrswerte über Diffserv-Netzwerke, 837
Verkehrsmanagement
Bandbreite regulieren, 829
Fluss steuern, 833
Netzwerktopologien planen, 843
Verkehr weiterleiten, 836, 837, 838
Verkehrswerte priorisieren, 830
Verkehrssteuerung, über die Metermodule, 833
Verlegung, auf Hosts mit einer Schnittstelle, 138
Verlorene oder abgeworfene Pakete, 41, 233
Vermittlungsschicht (OSI), 39
Vermittlungsschicht (TCP/IP)
ARP-Protokoll, 41
Beschreibung, 39, 40
ICMP-Protokoll, 41
IP-Protokoll, 40
Verschlüsselungsalgorithmen
für IPsec angeben, 600
IPsec
3DES, 523
AES, 523
Blowfish, 523
DES, 523
Version-Label, 746, 765
Verzeichnisname (DN), für Zugriff auf CRLs, 640
Verzeichnisse
/etc/inet, 609
/etc/inet/ike, 609
/etc/inet/publickeys, 663
/etc/inet/secret, 609
/etc/inet/secret/ike.privatekeys, 661
PresharedKeys (IKE), 660
Private Keys (IKE), 661
PublicKeys (IKE), 663
Zertifikate (IKE), 663
Virtual LAN (VLAN)-Geräte in einem
IPQoS-Netzwerk, 915
Virtual Private Networks (VPNs)
IPv4-Beispiel, 560-570
IPv6- Beispiel, 570-576
mit dem routeadm-Befehl konfigurieren, 561
mit IPsec schützen, 560-570
mit IPsec-Tunnel im Transportmodus
schützen, 576-583
Virtuelle private Netzwerke (VPNs), mit IPsec
erstellt, 527
Virtuelle private Netzwerke(VPNs), Konfigurieren mit
dem Befehl routeadm, 582
VLAN
Beispielszenarios, 167
Definition, 152-154, 167-173
in Solaris 10 1/06 unterstützte
Schnittstellentypen, 171
Konfiguration, 167-173
Physikalischer Anschlusspunkt (Physical Point Of
Attachment, PPA), 154, 169
Planung, 170
statisch
unter Solaris 10 3/05 konfigurieren, 153-154
Switch-Konfiguration, 168

VLAN *(Fortsetzung)*
Tag-Header-Format, 153
Topologien, 167-170
unter Solaris 10 3/05 konfigurieren, 152-154
virtuelles Gerät, 154
Virtuelles Gerät, 171
VLAN ID (VID), 152, 168-170
Voraussetzungen für IPMP, 783-784
VPN, *Siehe* Virtual Private Networks (VPNs)
VPN mit IPsec schützen (Übersicht der Schritte), 557-591

W

Webserver
für IPQoS konfigurieren, 866, 867, 877, 878
mit IPsec schützen, 539-542
Weitverkehrsnetz (WAN)
Internet
Domain-Namen-Registrierung, 38
Wrappers, TCP, 147

Z

Zeitmarken, 747, 767
Zertifikat-Anforderungen
auf Hardware, 637
verwenden, 662
von CA, 631
Zertifikate
anfordern
auf Hardware, 637
von CA, 631
Beschreibung, 632
CRLs ignorieren, 634
IKE, 607
in `ike/config`-Datei, 638
Liste, 627
selbst-signierte erstellen (IKE), 625
speichern
auf Computer, 624
Speichern
auf Hardware, 608, 651
Zertifikate *(Fortsetzung)*
speichern
IKE, 663
von CA, 632
von CA auf Hardware, 640
zu Datenbank hinzufügen, 632
Zielsystem, in IPMP
Definition, 783
Konfiguration in einem Shell-Skript, 807-808
manuell konfigurieren, 807
Ziffern, *Siehe* Verschlüsselungsalgorithmen
Zone-Datei, 214
Zonen
IPsec und, 529, 535
Schlüsselmanagement und, 535
Zufallszahlen, mit dem Befehl `od` erzeugen, 615